University of Zurich[UZH]

Department of Informatics

Electronic Data Safes –
Personal Information Management at the Intersection of Electronic Process Support and User-Managed Access in E-Business and E-Government

Dissertation submitted to the Faculty of Business,
Economics and Informatics
of the University of Zurich

to obtain the degree of
Doktor der Wissenschaften, Dr. sc.
(corresponds to Doctor of Science, PhD)

presented by
Joachim Pfister
from Germany

approved in July 2017

at the request of
Prof. Dr. Gerhard Schwabe
Prof. Dr. Jörn von Lucke

The Faculty of Business, Economics and Informatics of the University of Zurich hereby authorizes the printing of this dissertation, without indicating an opinion of the views expressed in the work.

Zurich, July 19, 2017

Chairwoman of the Doctoral Board: Prof. Dr. Elaine M. Huang

To my mother Katharina who missed the beginning and
my father Anton who missed the end of this journey.

“I know you're living in my mind.
It's not the same as being alive.
Supersymmetry.“
(Arcade Fire, Supersymmetry)

Abstract

In private households, paper-based documents are increasingly substituted by electronic documents. In order to "get organized", an individual nowadays needs to oversee a plethora of digital and physical information items stored at various locations. As a technological solution to alleviate or overcome this problem of information fragmentation, cloud-based storage services such as Electronic Data Safes (EDS) emerge as the quasi-natural habitat for all digital valuables. Besides storing such information items, an (active) EDS also connects individuals and organizations from the private and the public sector to exchange information items related to business processes following the user-managed access paradigm. This means, that the individuals decide with whom they want to share specific information items. In other words, an EDS acts as a tool or service at the intersection of personal information management and process support in the domain of e-government and e-business.

This thesis investigates the overarching research question: *How can we reduce or even overcome information fragmentation in the context of e-business or e-government processes?* by putting the EDS concept into practice. This is done by researching existing EDS services and by carrying out exploratory research using the prototype of an active EDS. Thereby, this thesis contributes to e-government, e-business, and human computer interaction by providing new knowledge and insights due to an in depth-analysis of current practices and by uncovering challenges and requirements that are relevant for the future design of EDS solutions or cloud-based information item storage solutions in general.

The thesis consists of four research essays. The *first essay* gives an overview of the current landscape of electronic data safes in the e-business and e-government domain. Thereby, and with its in-depth study of business models for EDS, this essay provides the foundation and context for the further research activities of this thesis.

Essays two and three identify current usage patterns and emerging problems from the user-perspective when individuals chose to store their information items in an EDS. The *second essay* investigates what it means to go paperless with the help of an EDS in terms of user-behavior. A typology of content that is kept safe in an EDS is developed. Moreover, the users' motivations are reflected and an EDS's role with respect to other cloud-based storage services is analyzed. Also, the challenges of maintaining a digital, personal archive are depicted and "data value zones" are introduced as a sensitizing concept to reflect upon problematic areas.

The *third essay* focusses on the aspect when digitally stored information items eventually become a digital legacy and which strategies people choose to shape and give access to it. Pre-mortem password sharing is identified as a common coping strategy. Additionally, the challenges associated with passing on a digital legacy, such as the lack of enculturated practices, difficulties in the appraisal and selection of information items, the preference for deletion, and implicitly transferring data stewardship duties are described and discussed to suggest design implications.

The *fourth and last essay* reports on the results of an evaluation of an EDS prototype with e-government and e-business process support in order to identify potential benefits, challenges, and problems. Four barriers for the adoption of an active EDS in the light of transformational government are identified: (1) offering citizens unfamiliar services that have the character of experience-goods; (2) failing to fulfil common service expectations of the customers; (3) failing to establish contextual integrity for data sharing, and, (4) failing to establish and run an (active) EDS as a multi-sided platform providing an attractive business model. Furthermore, design implications are suggested to overcome the identified challenges and problematic areas.

The *last chapter* wraps up the findings from the four essays and puts them into context with smart government initiatives aspiring to the idea of "government 4.0" or "industry 4.0" that are being discussed as emerging future topics.

Zusammenfassung

In Privathaushalten werden Papierdokumente zunehmend durch elektronische Dokumente ersetzt. Daher muss man heutzutage, um sich selbst zu organisieren, eine Vielzahl von digitalen und physischen Informationsitems, die an verschiedenen Orten gespeichert sind, im Blick behalten. Um dieses Problem der zunehmenden Fragmentierung von Informationsitems zu lindern oder gar zu lösen, bieten sich als technische Lösung elektronische Datensafes (EDS) an, die per se als quasi-naturgegebener Aufbewahrungsort für sämtliche, digitale Wertsachen fungieren. Neben dem Speichern von Informationsitems verbinden (aktive) EDS zudem Individuen und Organisationen aus dem privatwirtschaftlichen und öffentlichen Sektor, um Informationsitems für Geschäftsprozesse mit der Erlaubnis des Datenbesitzers auszutauschen, was mit user-managed access bezeichnet wird. Dies bedeutet, dass Individuen entscheiden, mit wem sie ihre eigenen Informationsitems teilen wollen. Man könnte auch sagen, dass ein EDS an der Schnittstelle zwischen persönlichem Informationsmanagement und Prozessunterstützung im Bereich von E-Government und E-Business liegt.

Diese Arbeit untersucht die übergreifende Forschungsfrage: *Wie kann die Fragmentierung von Informationen vermindert oder sogar verhindert werden im Kontext von E-Business oder E-Government*, indem man das Konzept eines EDS in der Praxis umsetzt? Antworten auf diese Frage werden dadurch erarbeitet, dass bestehende EDS-Dienste untersucht werden und zudem ein Prototyp zur Durchführung von explorativen Nutzertests herangezogen wird. Diese Arbeit leistet einen Betrag zur Forschung in den Bereichen E-Government, E-Business und Mensch-Maschine-Interaktion, indem neues Wissen und Einblicke generiert werden, beispielsweise durch die tiefgehende Analyse von gegenwärtigen Praktiken und durch das Ermitteln von Herausforderungen und Anforderungen, die für das Service-Design von zukünftigen EDS oder generell Cloud-basierten Speicherdiensten für Informationsitems von Nutzen sind.

Diese Arbeit besteht aus vier in sich abgeschlossenen Essays. Der erste Essay vermittelt einen Überblick über die aktuelle Landschaft von elektronischen Datensafes im Bereich von E-Business und E-Government. Dadurch und mittels einer detaillierten Untersuchung von Geschäftsmodellen für EDS schafft der Essay die Grundlage und den Kontext für die darauf aufbauenden Forschungsaktivitäten im Rahmen dieser Arbeit.

Essay zwei und drei widmen sich den gegenwärtigen Nutzungsmustern und den möglichen Problemen aus Endnutzersicht, die sich aus dem Einsatz von EDS beim Speichern von Informationsitems von Privatleuten ergeben. Der *zweite Aufsatz* untersucht das Nutzerverhalten beim Versuch, mittels eines EDS privat ein papierloses Dasein anzustreben. Als Ergebnis wird eine Inhaltstypologie von Inhalten in einem EDS vorgestellt. Zudem wird die Motivation der Nutzer reflektiert und die Position eines EDS im Informations-Ökosystem mit anderen Cloud-basierten Speicherdiensten beleuchtet. Ausserdem werden die Herausforderungen beschrieben, ein digitales, persönliches Archiv zu schaffen und „data value zones" (Zonen mit spezifischem Wert für Daten) werden als ein sinnstiftendes Konzept eingeführt, um Problematiken zu reflektieren.

Der Hauptfokus des *dritten Essays* liegt auf dem Aspekt des digitalen Vererbens, d.h., was passiert, wenn digitale Informationsitems zum digitalen Nachlass werden und welche Strategien von den Nutzern verfolgt werden, um ihren Nachlass zu schnüren und den Zugriff darauf zu ermöglichen. Das Teilen von Passwörtern vor dem Tode wurde als verbreitete Kompensationsstrategie identifiziert. Zudem werden die Herausforderungen beschrieben, die mit der Weitergabe eines digitalen Nachlasses verbunden sind, wie z.B. das Fehlen von traditionellen Handlungsmustern, Schwierigkeiten bei der Auswahl und Bewertung von Informationsitems, dem Wunsch nach Löschen und der implizit erteilten Verpflichtung an Dritte, sich um den Datennachlass zu kümmern. Zudem werden daraus auch Designimplikationen abgeleitet.

Die Evaluation und die Ergebnisse eines Prototypen eines EDS zur Unterstützung von Prozessen im E- Government und E-Business werden im

vierten und letzten Essay dargestellt. Es werden potentielle weitere Nutzenfaktoren, Herausforderungen und Probleme ermittelt. Vier Barrieren für das Erzielen von transformationellem Governments bei der Verwendung von aktiven EDS werden aufgezeigt: (1.) Bürgern werden ungewohnte Diensten bereitgestellt, die den Charakter von Erfahrungsgütern haben; (2.) Das Nichterfüllen von üblichen und verbreiteten Erwartungen von Kunden für die Dienstabwicklung; (3.) Das Verletzen der kontextuellen Integrität beim Teilen von Daten; (4.) Das Scheitern, einen (aktiven) EDS als multi-sided Plattform und mit einem attraktiven Geschäftsmodell zu schaffen. Es werden zudem Designimplikationen vorgeschlagen, um diese identifizierten Herausforderungen und Problembereiche zu adressieren.

Im *letzten Kapitel* dieser Arbeit werden die Ergebnisse dieser vier Essays im Kontext des Zukunftsthemas „Smart Government“ diskutiert, das auf Ideen von „Verwaltung 4.0“ und „Industrie 4.0“ fusst.

Acknowledgements

A PhD endeavor is like embarking on a journey into the dark unknown and finally emerging into the light. Having mastered this journey and its experience, I wonder which iconic songs, that I had listened to during that time, are forming the soundtrack to this thesis and which tonality it finally has. Is it a *bitter sweet symphony* (The Verve), a song about the *afterlife* (Arcade Fire) or just a *new error* (Moderat)? In the midst of the journey, it felt like *it's never over (hey Orpheus)* (Arcade Fire) or *circles* (Hooverphonic) because everything seemed harmonic but unfitting like *salt silver oxygen* (Anthony and the Johnsons) or incomprehensible like *Sæglópur* (Sigur Rós) of which *we've got a lot* (Sarah Neufeld) – leading to dreams about escaping like a *dragonfly* (My brightest diamond). Eventually, a tipping point was reached *wenn es passiert [when it happens]* (Wir sind Helden) and *alles [all]* (Wir sind Helden) will fit magically together which in its individual parts seemed *kaputt* (Wir sind Helden) for a while. In the end, the protagonist is moving from the *present tense* (Radiohead) into the future and is now *ready to start* (Arcade Fire).

My first words of thankfulness for accompanying this journey go to Prof. Dr. Gerhard Schwabe who accepted me as a doctoral student in his research group and supervised this work. He served as the midwife for the project "Data Purse – Data Management for Citizens" which funded vast parts of this PhD thesis journey and helped to put me into contact with valuable resources and people. Further thanks go to the Swiss Commission for Technology and Innovation (KTI/CTI) for funding the project as well as to all involved industrial partners from numerous private and public-sector organizations and their project representatives. My special thank goes to the overall project lead Benno Häfliger with whom I enjoyed collaborating very much and who glued together people and organizations. Furthermore, I am deeply thankful to Dr. Tobias Christen, Stephan Hopmann, and Dr. Francisco Jent who helped me in recruiting the participants for my interview study. And of course, many thanks to all the interviewees who shared their personal information management

experiences and practices openly. My sincerest thanks for building the initial prototype of the "Data Purse Portal" as an electronic data safe go to the (now happily graduated) Master's students Alessandro Peduzzi and Daniel Reber. Furthermore, I would like to thank Prof. Dr. Jörn von Lucke for acting as the co-reviewer of this thesis.

My socio-technological thanks are gleefully extended to my current and former colleagues in the information management research group who served as road warriors on the same and parallel tracks into the (un)known. Thank you (in alphabetical order): Erik, Mateusz, Mehmet, Mila, Peter H., Peter R., Philipp, Raffaele, Robinson, Susanne, Tobias, and Tom. And my "socio-administrative" thanks are dedicated to all other PhD students, post docs, (former) staff members and administrative members of the Ifi (Department of Informatics) with whom I enjoyed to work, had lunch, or met on various occasions intra- and extra-Ifi-muros.

And thank you for spending time, and/or food, and/or drinks together (in alphabetical order and grouped by location): Alice R., Anita & Remigi, Anja K., Carole & Adrian, Claudio S., Corinna S., Doro R., Flory & Ionut, Franzi L., Iris H., KuHuAuA, Lucia & Werner, Marc & Steffi, Manuel, Mark & Dave, Martina K., Michael F. Monika Z., Nicole S., Roberto L., Stefan A., Tine, Tobias & Thomas, and everyone in the Contrapunto choir.

I am indefinitely grateful for having had such great parents throughout all the years with their generosity, wisdom, compassion, and love – feeling very sad because they will not be able to read this anymore. My special thanks are dedicated to my aunt Irene for being there in the darkest hours in my life in December 2016 and keeping a vivid interest and caring attitude for me as newly orphaned PhD particle in this universe. Last, but not least, I deeply thank my supersymmetric PhD particle and partner in crime Werner for navigating together through time and space – thanks for being (there).

Contents

Abbreviations

AEDS	active electronic data safe
BMC	business model canvas
CST	customer
DC	design challenge
DI	design intervention
DSR	design science research
EBPP	electronic bill presentment and payment
EDS	electronic data safe
e-business	electronic business
e-government	electronic government
eID	electronic identity
eIDMS	electronic identity management systems
eSafe	electronic safe
FC	focal company
HIOB	human information organization behavior
ICT	information and communication technology
OS	operating system
MSP	multi-sided platform
PHR	personal health record
PIC	personal information collection
PIM	personal information management
PP	platform partner
PSI	personal space of information
t-government	transformational government
SBMC	service business model canvas
TMSC	transactional model of stress and coping
UTAUT	unified theory of acceptance and use of technology
WTP	willingness-to-pay

"If you have a reputation as a big,
stiff bureaucracy, you're stuck."

Jack Welch, former CEO of General Electric

1 Synopsis

1.1 Introduction and Motivation

Today, the majority of people in modern societies is accustomed to use electronic interfaces to interact with services, either on a volunteered basis or forced by a myriad of external factors (for example, economic incentives, professional or peer group pressure etc.). Besides the electronic world, each of us is still anchored in the physical world where paper documents, nevertheless, are needed to exchange information due to various practical, organizational, and legal reasons. We all have to deal with various kinds of information items (Jones 2012) which accumulate in our personal space of information (PSI) where personal information collections (PICs) as islands of relative structure and coherence exist (Jones and Teevan 2007a). The tremendous growth of data storage offerings (offline and online) as well as an increase in already digital born data sources (digital photographs, music, electronic documents etc.) are reinforcing the tendency to keep everything and therefore defer difficult keeping-decisions (Kim 2013; Marshall 2011).

Nowadays, it is almost commonplace to own several digital devices that are used alternatingly or simultaneously to create and access digital information items. Furthermore, every one of us interacts with various service providers which entails questions such as: Do you still know on how many web sites/services you are registered with and which data you provided for signing up? Do you check your utility or telecommunication provider's portal for your new bill on a regular basis? When you move, do you surely know whom to inform about your new address? These small

vignettes show that information fragmentation (Karger 2007) is a common problem that will keep flourishing: We all will have to take more and more decisions on finding, keeping, managing and (re-)using once encountered information items which is multiplied by the increasing number of devices and services that we are interacting with. Moreover, we will have to bridge and master the digital and the paper-based worlds in order to manage one's life if we inevitably engage in governmental or business processes and transactions. Now, the question arises, how information technology and new services might help to overcome the problem of information fragmentation. This PhD-thesis explores the relationship and potential areas of tension of personal information management (PIM) and process support in the light of information fragmentation. Individual behavior will be analyzed, how people use their individually structured PSI and how they might be supported in exchanging information items with e-government and e-business service providers using an electronic data safe (EDS) in order to overcome or reduce the problem of information fragmentation. An EDS is a cloud-based storage service for the management of personal information items and their controlled sharing with e-business or e-government processes under the user-managed access paradigm. In the following chapters, background information and related work will lay the grounds for presenting the research questions and the approach taken to answer them.

1.2 Problem Statement

Since service providers have better IT support for managing the whole customer life-cycle and they have better support for tracking processes and transactions, there is an imbalance disfavoring the customers. In order to manage their life, customers have to get into contact with several service providers, for instance health insurance providers or public authorities to carry out voluntary (e.g. marriage) or involuntary transactions (e.g. tax declarations). For managing their social life, people have IT support through social networks (such as Google+ or Facebook). Their professional life can be managed by other social networks (such as

LinkedIn or XING). These services can be considered as hubs specialized in the management of a certain aspect of a person's life. However, such a hub for supporting and carrying out generalized, "administrative" tasks with public authorities or business organizations is lacking. People are left to their (multitude) of own devices, information items and service providers, and, thus, apply their own PIM strategies to cope with the ever-growing information fragmentation.

Customers and citizens are offered many channels to interact with a service, for instance via a customer portal. Each of these portals needs to be remembered, configured the right way to receive notifications via e-mail, and to be checked on a regular basis – separately for each service provider. This imposes a huge cognitive burden on individuals as they have to actively manage a universe of fragmented service providers. PIM tools like password managers could be used to achieve a unified view of a person's account credentials. But the majority of people (a finding gathered from interviewing citizens about their PIM behavior, performed in the context of this PhD thesis) does not use such tools. They either use the same or variants of the same passwords or they rely on password recovery mechanisms – if they still remember that they have registered for a certain service. Framing cognitive burden as a consequence of information fragmentation gives rise to potential explanations of observed behavior: For instance, people seem to dislike checking a service provider's portal on a regular basis, unless high frequency task like executing payments can be carried out there because visiting a portal just for one task creates cognitive burden. Moreover, e-mail messages are nowadays frequently used to signal changes in a process' status to the customers. But for security reasons the messages are formulated quite neutral which creates the need to consult the service provider's portal which, again, induces cognitive burden. Furthermore, if processes need to be supplied with an individual's information items that are stored in a fragmented PIC, the retrieval of these items and their packaging according to a service provider's specification (e.g. by completing forms) induces further cognitive burden. This leads to the overarching research question of this thesis:

RQ0: How can we reduce or even overcome information fragmentation in the context of e-business or e-government processes?

To achieve this, I propose that we should follow the concept of an EDS or a "life management platform" in which PIM and process support are combined (for example in the e-government and e-business domain). This alleviates the cognitive burden on how to cope with information fragmentation.

1.3 Research Questions

In order to answer the overarching research question *RQ0 "How can we reduce or even overcome information fragmentation in the context of e-business or e-government processes?"* two (sub-)research questions need to be answered. The first research question provides the formative background and is stated as follows:

RQ1: What is the nature of the practices that people exhibit in order to manage information items related to their personal, administrative life?

This research question aims at identifying the current pains and problems people have when they are managing their paper-world and digital information items. People have many different information items stored physically or electronically. Yet, we do not know which of these information items are of importance and if this translates into specialized keeping strategies – especially if these information items shall be used in processes, for example, statements and invoices to be attached to a tax declaration.

Much research has been done in the area of human information behavior (Case 2007), dealing with the process of encountering new, unknown information. On the contrary, little research is dealing with "human information organization behavior" (HIOB) that focuses on organizing once encountered information (Cole and Leide 2006; Spurgin 2008). By answering the first research question, I will be able to contribute new

knowledge to close this gap. The findings (identified problems and current practices) can also be used to inform the design of services offered in electronic data safes or life management platforms – or cloud-storage services in general.

The results are then used to inform the prototypical design of a solution (electronic data safe) to analyze if information fragmentation can be reduced or even overcome. This is related to the second research question:

RQ2: How can we support the exchange of information items via electronic data safes in order to reduce or even overcome information fragmentation?

If the interaction between an individual and an organization takes place through online-assisted processes, an electronic data safe will serve as a "data transaction platform" (Breitenstrom et al. 2008; Schulz et al. 2010). In this sense, an electronic data safe can be interpreted as a boundary object (Star and Griesemer 1989) that connects an individual's personal space of information (the paper and electronically based universe of all information items) with an organization's space/universe of information.

By answering research question two, the following contributions are delivered: First, user's perceptions about the idea of coupling personal information management with process support will be revealed and reflected. Second, essential or useful components of an electronic data safe or life management portal are identified. Thus, an evaluation of a prototypical electronic data safe as a design solution will be carried out trying to answer if the envisioned solution helps to overcome the information fragmentation problem and which effects the solution created.

1.4 Structure of this Thesis

This thesis consists of four essays that are based on peer-reviewed conference articles. Each of the essays answers a distinct research question

and contributes to answering the research questions (see also Table 1) as stated in chapter 1.3.

The *first essay* gives an overview of current trends of electronic data safes in the e-business and e-government domain and provides the foundation and context for the further research activities in this thesis. The *second and the third essay* identify current usage patterns and emerging problems from the user perspective when individuals chose to store their information items in an EDS. The *fourth and last essay* reports on the results of an evaluation of an EDS prototype with e-government and e-business process support in order to identify challenges and problems. The *last chapter* wraps up the findings from all essays and puts them into context with smart government initiatives aspiring to the ideas of "government 4.0" or "industry 4.0" that are discussed as emerging topics.

Chapter	Title	RQ
1	Synopsis	
2	Essay 1: The Landscape of Electronic Data Safes	RQ2
3	Essay 2: Current Usage of an EDS	RQ1
4	Essay 3: The Challenges of Shaping a Digital Legacy in Presence of an EDS	RQ1
5	Essay 4: Active EDS and Transformational Government – Evaluation of a Prototype	RQ2
6	Outlook: EDS as an Infrastructure for Smart Interactions	

Table 1: Structure of the thesis

1.5 Methodology

In Information Systems research, two research paradigms are prevalent: (a) behavioral science and (b) design science (Hevner et al. 2004). This

thesis follows an explorative research paradigm with the goals of discovering and describing "[...] unexplained phenomena, their correlates, and the contexts in which they manifest." (Briggs and Schwabe 2011) For these exploratory research activities, which are ascribed to the design science research paradigm, behavioral methods such as qualitative interviews with sense-making methodologies such as grounded theory (Glaser and Strauss 2009; A. L. Strauss and Corbin 1998) or thematic analysis (Braun and Clarke 2006) can be used.

In this PhD thesis, therefore, the essays two and three focus on describing and explaining user behavior and putting it into context with existing theories (for example, information ecologies and the transactional model of stress and coping) following the behavioral science approach. The first essay of this thesis uses document analysis and qualitative interviews to explore the current landscape of electronic data safe solutions resulting in a contextual description of the environment where the phenomenon of interest (information fragmentation with PIM activities for e-business and e-government transactions) occurs. Finally, the fourth essay is moving into the direction of design-science-oriented exploratory research by using a prototype as an artifact to explore user's reactions. Nevertheless, behavioral science research methods are used to interpret user's reactions that were provided in the qualitative interviews in this fourth essay.

When behavioral science methods, such as thematic analysis, are used in this thesis, I proceeded in a data-driven fashion without establishing assumptions about an "a priori understanding of the situation" (Orlikowski and Baroudi 1991, p. 5). Thus, I followed an interpretive research paradigm based on an epistemological understanding that the knowledge of the world is socially constructed – in contrast to a positivist research stance which would assume that there is an objective reality.

1.6 Background and Related Work

This chapter gives background information and points to related work. After having presented information fragmentation as the phenomenon

of interest, the concept of "electronic data safes" and "life management platforms" will be portrayed. These technological solutions or concepts are assumed to assist individuals to reduce or even overcome information fragmentation. Both concepts combine components and functionalities for PIM and process integration which constitute the intersection of all the research activities on which this PhD thesis is based.

1.6.1 Information Fragmentation

Information fragmentation is defined by Tungare (2009) as: "[...] the condition of having a user's data in different formats, distributed across multiple locations, manipulated by different applications, and residing in a generally disconnected manner." Reasons for this fragmentation are (1.) that applications are only designed around a single, fixed data type, and (2.) that there is a lack of integration among tools and mostly proprietary data formats exist (Van Kleek 2011). Prior research projects have dealt with the information fragmentation problem. The first to mention is Haystack (Karger et al. 2005) which is a semantic desktop application that unifies information items from multiple source applications through linking them via RDF. In the Haystack project, the focus is on the integrative aspects of user interface and a smart representation of data in its context thus eliminating information fragmentation. Second, the Gnowsis-Project (Sauermann 2009) and its successor NEPOMUK (Groza et al. 2007) are aiming at creating the social semantic desktop. Third, there is the project called Planz (Jones and Anderson 2011) which provides a document-overlay to existing storage systems to support project-based information item organization.

1.6.2 Personal Information Management

How persons keep, organize, and use information items has been studied in the domain of Personal Information Management (PIM) (Jones 2012, 2013, 2015, 2008; Jones and Teevan 2007b). As a research field, it is very interdisciplinary because PIM activities are not bound to a specific tool or device but have to be put into a broader context of a "[...] person's integrative use of information across tools and over time." (W. Jones & Ross,

2007, p. 472). It differs from information behavior research because models on information behavior, for example, Wilson's (2000) second model, focus more on how to encounter new information: "However, all these models talk only about how public information is found and ignore what happens after finding has occurred." (Whittaker 2011, p. 4)

PIM is defined as (Jones 2012, p. 3): "[...] both the practice and study of the activities a person performs in order to locate or create, store, organize, maintain, modify, retrieve, use and distribute information in each of its many forms (in various paper forms, in electronic documents, in email messages, in conventional Web pages, in blogs, in wikis, etc.) as needed to meet life's many goals (everyday and long-term, work-related and not) and to fulfill life's many roles and responsibilities (as parent, spouse, friend, employee, member of community, etc.)." The body of literature on PIM gives valuable insights, for example how people use their electronic folders (Bergman et al. 2010; Henderson 2009), what problems arise if documents are shared over several devices (Dearman and Pierce 2008), or when cloud storage services are used (Marshall and Tang 2012), and if users exhibit a kind of preparatory behavior, for instance, by sorting documents into folders for an anticipated later use (Whittaker 2011).

Existing research on information organization behavior tends to focusses on PIM activities in specific contexts such as work (Malone 1983) or the professional home office (Thomson 2013), populations such as academics (Kaye et al. 2006) or engineers (Hicks et al. 2008), across devices (Boardman and Sasse 2004; Dearman and Pierce 2008) or about the use of (personal) cloud-based storage (Capra et al. 2014; Marshall and Tang 2012; Odom, Sellen, et al. 2012; Tang et al. 2013). As an exception, the recently published study by Vertesi et al. (2016) takes a very general approach to answer the question "How do people manage their personal data?" which was motivated by the claim of Barkhuus (2012) that findings are often bound to the context of a study and that taking a broader perspective would generate new insights. Therefore, these authors took a general view on the PIM practices and the ecosystems that people engage in to manage their information items. They

placed their findings in the wider context of a "moral economy". In doing so, they report on a set of practices, the cultural expectations, affects and responsibilities that arise when people are confronted with a heterogeneous information ecology landscape.

PIM activities are not only dedicated to manage hot (immediate) or warm (working) information items (cf. Sellen and Harper 2002) but they also include information items not longer in use. Whittaker (2011) suggested different information properties that influence how information items will be curated: (a) action-oriented items require the user to do something *(action-orientedness)*, (b) informative items do not require a user to act *(informativeness)*, and (c) the *uniqueness* of an information. Nevertheless, it is very hard to assess the value of an information item's future worth (Marshall 2007), especially if they do have certain values which change over the "life-cycle" of the item itself and with respect to their owner (Marshall 2011). Since storage costs are inexpensive, the default is to keep all these digital items: "In our analog past, the default was to discard rather than preserve; today the default is to retain." (Mayer-Schönberger 2007, p. 4) And, "[...] there is no Nobel Prize or Oscar awarded for maintaining a neat, well-pruned file-system." (Marshall 2011)

Generally, personal information items are stored with the attitude of "benign neglect" ignoring the consequences or needs of "data stewardship" through deferral to somewhere in the future (Marshall 2007). The strand of research on personal archiving (Hawkins and Kahle 2013; Lee 2011; Marshall 2008a, 2008b) sheds light on these often implicitly occurring practices of forming a digital archive. The body of literature on personal archiving gives background on the motivation why and what people do archive – and how they struggle with it. Marshall et al. (2007) describe that "(1) digital materials accumulate in a different and more problematic way than physical materials; (2) personal digital belongings are fundamentally distributed on and among different computers, applications, and storage media.

Moreover, PIM-related research investigates the role of digital possession (Cushing 2012; Kaye et al. 2006; Odom, Sellen, et al. 2012; Watkins et

al. 2015) to understand what motivations exist to curate or create collections of information items. So far, to the best of our knowledge, no dedicated research has been performed in order to analyze how people manage "official" information items that had been directed to them, for example, through the use of e-government, e-business services, or just originating by the fact that you are alive and "officially" registered and bound by documents to this world (as the German saying goes: "From the cradle to the grave: forms everywhere."). With our research, we expand the literature on PIM regarding the question if such official documents are forming a distinct part of an individual's PSI and how they are organized, especially, if dedicated storage services like electronic data safes, as introduced in the next chapter, exist.

Information re-finding is different from finding new, unknown information (Deng and Feng 2011). Three main types of re-finding were identified (Elsweiler et al. 2011): lookup tasks (searching for a specific information item, for example, a password in an e-mail), item tasks (looking for a particular information item to pass and share it or use it for a given task), and multi-item tasks (more items are involved and the user has to collate information to complete a task). As these authors mention, "re-finding tasks can often be difficult, time consuming and frustrating." (Elsweiler et al. 2011). Not finding known items leads to disappointment (Slone 2000). Information fragmentation will even worsen all these problems. People already experience a loss of productivity through their daily need for searching information items which induces high search- and transaction costs. The tremendous growth in literature on "self-help" of getting better and more organized (like the famous approach of "Getting Things Done", Allen 2001) can be seen as a symptom of the inherent desire of people to "simplify your life" (as the best-selling book is titled, Küstenmacher 2004).

1.6.3 Process Support

Many tools and applications for managing one's personal information, like e-mail or to-dos, exist but only in a fairly disconnected manner, creating application and data silos. When information items have to be

sought and brought together for larger tasks, for example preparing an application for a new job and delivering it via a company's job portal or completing an online tax declaration, many information silos have to be consulted. The citizen or the individual is burdened with the whole integration effort without having the proper means of controlling the information items that were provided to processes and to keep track of a process' execution.

With the advent of the Internet, people and organizations are using this channel more and more for initiating e-business and e-government transactions and processes (TNS infratest 2012). In the domain of e-government, for example, Schwabe (2011) describes that electronic forms, standardized input and rule-based processing will lead to efficiency gains for public administrations and citizens. Additional value is created when information has to be provided only once and not several times. Schwabe (2011) claims that dynamically configured forms with rule-based error checking, ideally based on pre-defined life-events, will leverage the online-channel's full potential. Structuring information and services according to life-events (Müller 2011) is becoming a well-established practice and more and more administrations are embracing this structuring aid. Combining general life-events with citizen specific profiles and data will result in truly personalized services (AlSoud and Nakata 2011) that contribute to achieving a "one-stop government". The task at hand that citizens want to execute determines the choice of the channel (web based or still predominant telephone and face-to-face) (Ebbers et al. 2008), for example registering a civil marriage online is not regarded to be attractive (Barth and Veit 2011).

Exchange of information items in the context of e-business or e-government processes often takes place using Web forms. Completing forms is regarded as a tedious and repetitive action, as reported by Winckler et al. (2011). This motivated Winckler et al. to develop a solution that assists users in completing any web form with recurring patterns of information (for instance, address or bank account data; I will refer to these structured information items as "field data") that are drawn centrally from a PIM

system. I argue that this focus on "auto-complete" or "assisted-complete" might be feasible for providing field data but carrying out larger e-government or e-business transactions which involve the exchange of documents (for example photos to prove the possession of something or plans of real estate property) cannot be supported by such an auto-complete solution. EDS, as introduced before, will put users and their personal space of information in the center and allow them to share information items with a process, and, of course, to receive information items from processes, to keep track of their shared data, and they will be assisted throughout the execution of services, for example by providing to-dos and reminders.

Business process re-engineering methods are used to model an organization's processes in order to improve customer service and lower their transaction costs. When information items have to be exchanged in processes, an interface is needed to perform this information exchange. While the organization keeps track of a customer's or a citizens' input and current process state, the customer has been often left without further notice other than "Your request will be processed". E-business services nowadays often give detailed feedback on a process' or a transaction's status on their Web site. Process transparency is used to reduce information asymmetries (Nussbaumer and Matter 2011) in order to achieve customer satisfaction. Service providers have detailed knowledge about their customers and use many systems, for example, customer-relationship management systems, in order to get a holistic view on each customer (Bloching et al. 2012). On the other side, customers do not have such sophisticated tools which help them to manage all the data provided to the multitude of service providers, and which help them to keep track of their processes in which they are involved. They are left alone with their own personal information management, which may result in quite diverse difficulties and practices for managing their information items. This was also recognized in the domain of knowledge-management and process-oriented case-based reasoning by Görg and Bergmann (2015). These authors introduced and defined the term *social*

workflow as "[...] an executable process representation, serving private individuals and groups of people to fulfil their objectives by providing means to describe and link personal activities and data objects according to procedural rules." (Görg and Bergmann 2015, p. 2) Furthermore, they define a *social workflow service* as a service which "[...] provides a modelling and flexible execution service for social workflows addressing private individuals as users. This service includes means to organize, share, and reuse social workflows and the related workflow data within a virtual community of private users." (Görg and Bergmann 2015, p. 2) In their work, Görg and Bergmann suggest that supporting social workflows (such as planning to attend a concert with all steps involved from buying a ticket, travelling there and looking for accommodation) via IT artefacts in the private domain is the next step besides the already well-established business process management. Electronic data safes, as introduced in the following chapter, might serve as a platform to support social workflow services.

1.6.4 (Active) Electronic Data Safes

The projects dealing with information fragmentation presented in the previous chapter focus on the desktop and the applications running on a personal computer. Besides these, "personal data lockers" are emerging as technologies that shall help users to give them control over their data (Van Kleek et al. 2012). As an emerging topic, there are many parallel or slightly differing concepts and terms used nowadays: (personal) data lockers, personal data stores, (personal) data vaults (Brochot et al. 2015), or, as it will be used in this thesis, electronic data safes (EDS). Early works related to electronic document safes in the German-speaking e-government literature appeared as early as 2005 (von Lucke 2005, von Lucke 2008). Several authors argue that separating data storage from data usage will enable a true advancement for the current Internet (Mun et al. 2010; Van Kleek et al. 2012): „Instead of individuals sharing their personal data streams directly with services, we propose the use of secure containers to which only the individual has complete access." (Mun et al. 2010) Electronic data safes can be regarded as such infrastructures that provide data

sharing capabilities under the user-managed access paradigm and allow users to exert informational self-determination, and to gain transparency on how information is used (Andrieu 2010).

In this PhD-thesis, I will follow the definition of Breitenstrom et al. (2008) which was given in the domain of e-government (translated by the author of this thesis): *"An electronic data safe is a virtual data locker based on modern information and communication technologies which can be reached via electronic media in order to store, administer or share electronic data and documents."*

As an alternative definition for electronic data and document safes, the European Commission uses the following, thereby putting emphasis on the duality of document management and data management which is performed with the help of an electronic safe: *"An electronic data and document safe (eSafe) is a virtual repository for storing, administering and sharing personal electronic data and documents. It provides storage of and access to archived documents for authorized parties in secure manner and makes online transactions more efficient, comfortable and user friendly."* (European Commission 2012)

This apparent dichotomy or duality of data and documents is explainable by referring to the DIKW (data, information, knowledge, wisdom) pyramid or, in the German literature, the "knowledge staircase" (Wissenstreppe) introduced by North (2016). At the lowest level of the staircase, symbols are exchanged (for example, "010010011001"). When – alluding to semiotics – syntactical information is added to the symbols, data is exchanged (for example, "+414466688822"). Data is hardly interpretably on its own. By adding semantics, data becomes information (for example, "telephone number of Mrs. A: +414466688822"). Thereby, information items become understandable to humans. But the information items itself do not lead to insights or actions. Only if information items are linked to a context, experiences, and expectations (adding pragmatics) they transform into knowledge. Knowledge then becomes actionable by its application and the motivations to apply it. In information science,

this is formulated as "information is knowledge in action" (Stock and Stock 2013).

An electronic safe simultaneously contains data and information which are often formatted as documents as the primary representation for human readability and understandability. Documents can either contain only human readable information or they might also have attached machine readable information or data (or they can be transformed into these). In this thesis, I refer to the electronic safe as a service to manage data based on the foundational hierarchy of the knowledge staircase that documents consist of information items that, again, consist of data items, and ultimately of symbols. As suggested in the discussion of the concept of a "document" in information science (Stock and Stock 2013), the concept of "resources" would also be a synonym for documents. But with respect to common language usage of the words "documents" and "data", an "electronic resource safe" would be terminologically correct, too, but it sounds rather abstract. As another option, using the compound "electronic document safe" could be misunderstood as an implicit restriction that only well-formatted documents (like PDF files) might be only stored therein electronically and excluding data items. And using the compound "electronic information safe" might exclude the notion of being able to store documents therein. Therefore, I suggest using the compound "electronic data safe" to denote terminologically the concept's ability to store any kind of resource that is made up of data items. In consequence, all upper-level representations such as information items, documents and finally also knowledge items are then subsumed by referring to this more foundational term.

The owner (individuals, private or public sector organizations) of such an electronic data safe (Breitenstrom et al. 2008; Schulz et al. 2010) can securely store documents and data in the cloud and share it, based upon the individual's decision, on a fine-grained level with other parties. For example, citizens will be able to share data from their electronic data safes with e-government processes and they can see and understand in which parts of a process their data will be used (Schulz et al. 2010). This

user-managed access paradigm is the central design principle of an EDS which means that the safe owners decide with whom and with which e-business or e-government processes they share their information items. If documents are transmitted entirely electronically, benefits from optimized processes with less manual errors due to changes in medium may be possible. Private sector organizations are also able to send data and documents to their customers via an electronic data safe. Together with all (mobile) devices, such as smartphones or tablet PCs, a "personal cloud" (Reed et al. 2011) will evolve.

An electronic data safe is more than cloud storage as offered, for example, by Dropbox, (formerly) Wuala, Microsoft SkyDrive/OneDrive, or Google Drive. Many of these offers do not provide encryption of the information stored (for a comparison of the security of cloud storage, see (Borgmann et al. 2012)) or a transfer of data to processes (Schulz et al. 2010). According to Schulz et al. (2010), electronic data safes will provide benefits to all types of users because data and document delivery from trustworthy senders, data sharing mechanisms on a fine-grained level, and tight integration into business processes are combined in one place. This thesis uses the term "active electronic data safe" (AEDS) in order to emphasize the process support capabilities that transcend mailbox-like document reception and storage. Thus, an AEDS serves as an "one-stop-shop" (Kohlborn et al. 2013; Wimmer 2002), i.e. an individual's single contact and interaction point for information items and processes related to organizations from the public and the private sector.

Figure 1: (Active) Electronic data safe as an intermediary

(A)EDS are also evolving from portals (von Lucke 2007, von Lucke 2008) and plain document storage solutions to an infrastructure component for user-managed information and process management for which the term

life-management platforms has been coined (Kuppinger 2012a, 2012b; Kuppinger and Kearns 2013). They act as an intermediary replacing many point-to-point-connections and they serve as a multi-sided platform (MSP) to connect individuals and organizations – both, from the private and the public sector (Brunzel 2011) (see Figure 1). To carry out transactions in business processes, this exchange of information items happens via "plugins" with respect to the original concept of an EDS or with "apps" with respect to the concept of a life-management platform. The stakeholders are the individuals/citizens, the service-providers/organizations and the platform of the (A)EDS/life-management platform itself.

1.6.4.1 EDS as a Platform and a Network Good

Connecting the public and private context via a MSP in the e-government context was diagnosed as an embryonic research area (Bharosa et al. 2013). The simultaneous use of an infrastructure component, such as an AEDS, by the private and public sector makes sense because one organization alone often has too few customer contacts in order to justify the development and maintenance of such an infrastructure. For example, a German citizen is said to have one to two contacts with the public administration per year (Lenz 2001). AEDS are a network good: The more organizations offer services on an AEDS' platform, the more attractive it will become for customers – and vice versa. Postal services or telecommunication providers who consider themselves as established and natural intermediaries are complementing their portfolio of electronic document delivery solutions, for example, by providing electronic payment, authentication or secure storage for individuals and organizations (Finger et al. 2014), thus, also moving into the direction of AEDS. Nevertheless, these classic intermediaries often stick to a document-centric "mailbox" metaphor which is extended in the AEDS' vision by process support capabilities or value-added services to assist in personal information management tasks.

1.6.4.2 EDS in E-Government

On a European level, the concept of an EDS also gained traction in the context of research programs such as "ISA²" (Interoperability solutions for public administrations, businesses and citizens) (European Commission 2016a) with the specialized sub-action "Interoperability Agreements on Electronic Document and Electronic File (2016.26)" (European Commission 2016b). This action aims at providing an overview of solutions and standards for electronic documents and files. Within this action, a "Detailed analysis of e-Safe and e-Document solutions in Member States and EU initiatives" was elaborated but has not been published yet officially (European Commission 2016c). Thus, the European Commission has recognized the importance of providing mechanisms to support the management of electronic documents as a foundation for expanding e-government. Electronic safes (or eSafes) have been diagnosed as one of five key enablers that are a pre-requisite to assess the eGovernment performance of the EU's member states. Besides eSafes, other key enablers were identified: electronic identifications, electronic documents, authentic sources, and Single Sign On capabilities. Nevertheless, the eSafe component had the lowest benchmark score with 35% compared to an electronic identity with a benchmark score of 62%. This was diagnosed as an obstacle to achieve "advanced, transactional, automated services." (European Commission 2014)

In the yet unpublished study "Detailed analysis of e-Safe and e-Document solutions in Member States and EU initiatives" (European Commission 2016c), the European Commission identified seven categories of e-document and eSafe solutions based on their functions. For the sake of completeness, I will report on these categories. Such a functional categorization helps to cluster eSafe solutions, but nevertheless, it should provide room to accommodate for a service's development, for example, by embracing future developments and a service's gradual transition into other categories. While working on this thesis, for some services such an evolutionary transition was observable, for example, with the Austrian e-Tresor solution. The categories, as identified in the unpublished study

mentioned before, were: (a) machine to machine: These are solutions facilitating the exchange of data in the G2G context; (b) notification and dispatching: the government sends documents and notifications to citizens and businesses using a unified platform; (c) message box/e-delivery: citizens or businesses receive documents via a secured electronic mailbox as a registered electronic delivery service; (d) storage-only eSafe solutions (strong boxes): their aim is to provide safe and secure storage of documents without any transactional component; (e) eSafe solutions for bidirectional communication: these are services used by citizens and businesses to send and receive electronic documents – also with private entities. Sharing of electronic documents is also possible; (f) legislation/frameworks: concepts describing the desired architecture of e-government applications, and (g) web portals: web sites as information resources and documentation about national interoperability specifications. Using these categories, "electronic data safes", as understood in this PhD thesis, will fall into the categories of "notification & dispatching", "message box/e-delivery", "storage only eSafe solutions" and "eSafe solutions for bidirectional communication".

As we see, an (A)EDS is perceived as an IT-artefact helping to reduce information fragmentation and supporting processes in "social workflows". The overarching vision and aim in the context of e-government is to use technology as an enabler for deeper changes and transformations in the service-delivery from the government to its citizens or business clients. This train of thought culminates in the abstract aim of realizing a "transformational government" (t-government) which is defined by OASIS in its Transformational Government Framework Version 2.0 as: *"A managed, citizen-centric, process of ICT-enabled change within the public sector and in its relationships with the private and voluntary sectors, which puts the needs of citizens and businesses at the heart of that process and which achieves significant and transformational impacts on the efficiency and effectiveness of government."* (OASIS 2014) One of the key features of this shift is named "investing in smart data" to ensure that the government's digital assets are available on an open and interoperable basis. Customer-centricity is seen as the central design tenant of any strategic

and operational activity in order to render the whole government transformational and not just transforming it through technology (OASIS 2014). In the end of this PhD thesis, the findings of all the essays will be discussed to analyze the potential of an (A)EDS as an infrastructure component for t-government and smart government.

1.6.4.3 Fundamental Requirements and Business Drivers of EDS

In summary, electronic data safes are tools that help individuals to exert informational self-determination and to gain transparency on how information is used (Andrieu 2010). There are some fundamental requirements, electronic data safes have to fulfill (Breitenstrom et al. 2008):

(1.) guaranteed privacy that only the owner can access and share his or her data,
(2.) an adequate technological, organizational and legal framework to protect the privacy of personal data,
(3.) changing a service provider must not be complicated for end-users,
(4.) if several data safes exist, they should be manageable under a single integrated user interface,
(5.) sharing data and documents shall be supported by electronic identity management, and
(6.) retention periods and service-level agreements must be obeyed and supported.

Privacy-by-Design (Cavoukian 2009) will be essential in order to create trust in the service and its provider, for example, by providing transparency mechanisms. A user should be able to understand where and which information items are used by whom. This also relates to the need for process transparency (Nussbaumer and Matter 2011).

As business drivers for e-safe and e-document solutions, the unpublished report of the European Commission (2016c) reported upon the following: (a) reducing the costs for paper handling and postage; (b) improving e-government experiences by providing a single spot for managing official documents; (c) efficiency gains due to optimized transactions; (d)

supporting the concept of the "connected government" with a seamless data and information integration across branches of the public administration; and (e) the implementation of the "only once" principle which also reflects the idea of the "one-stop government" to avoid redundant data acquisition.

1.6.4.4 Predecessors of EDS: Infomediaries and VRM

In their position paper, Narayanan et al. (2012) give a short historical background on the development of personal data stores, starting in the late 1990ies with "negotiated privacy techniques". Especially the concept of infomediaries (coined by Hagel III and Rayport 1997) was identified as a predecessor of today's personal data stores: "We believe that consumers are going to take ownership of information about themselves and demand value in exchange for it." (Hagel III and Rayport 1997).

Infomediaries are companies that act as guardians of personal information. Furthermore, they serve as agents and brokers for the exchange of personal data, for example, to find the best match of an insurance company based on the needs expressed by the customer and managed by the infomediary. In doing so, the interaction and transaction costs of the consumers and service providers will be reduced (Hagel and Singer 1999). Moreover, the consumers would be protected from "the perils of asymmetric information and moral hazard." (Hagel and Singer 1999)

Three components are constituent for achieving the aims of an infomediary (Hagel and Singer 1999): (1.) a set of privacy tools to assist the customers in engaging in commercial transactions without requiring them to expose personal information; (2.) a set of profiling tools that will help individuals manage their profile and profile data; and (3.) services that will use the data provided by the individual's to maximize the value of the infomediary's clients. But within five years after the concept of infomediaries has been around in the press or worked upon in scientific contexts, this whole movement as well as all commercial companies (Persona, Privada, Lumeria and AllAdvantage) vanished (Narayanan et al. 2012). The reasons for failing were related to problems of (1.) providing

value to consumers and businesses at the same time, (2.) promoting infomediaries as trustworthy market participants, (3.) rising concerns about privacy, and (4.) achieve critical mass and gain first-mover advantages (Leickly 2004).

The idea of informational self-determination and receiving benefits and value in exchange for personal data continued in the "Project VRM" (Project VRM 2012), which forms a conceptual counterpart of the traditional customer relationship management that was now reformulated as "vendor relationship management". With the help of VRM-tools like electronic data safes or personal data stores, customers should be able to emancipate from service providers and "[...] bear their side of the relationship burden. [...] Customers will also be involved, as fully empowered participants, rather than as captive followers." (Project VRM 2012) Another predecessor for electronic data safes is the concept of a digital strongbox that was intended to support e-commerce processes and data and document exchanges (Hardjono and Seberry 1996).

The emerging concept of a life-management platform (Kuppinger 2012a) combines the personal data store/VRM-vision with process integration of electronic data safes. Life-management platforms will form an integrative solution that combine PIM (through electronic data safes) and process support. Such technological tools form part of a complex socio-technical system between individuals, service providers from the public or private sector, and data safe providers. From a research perspective, the technological and organizational instantiation of the concepts "electronic data safe" and life-management platforms will generate interesting end user reactions, and, as well, rich research opportunities.

1.7 Overview of the Essays and Their Contributions

The essays in this dissertation are based on four peer-reviewed conference articles. In the following, these essays and their contributions are detailed.

Citation	Pfister, Joachim and Schwabe, Gerhard (2013): „The Landscape of Electronic Data Safes and Their Adoption in E-Government and E-Business". In: Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS). January 7 – January 10 2013. Wailea, Maui, Hawaii., United States. 1963–1972, DOI: 10.1109/HICSS.2013.532.
VHB Ranking	VHB-JQ: C The HICSS e-government track is ranked as one of the top conference in the e-government domain (Scholl and Dwivedi 2014).
Type of Paper	Research paper
Aim	This paper reports on the concept of electronic data safes for managing personal data and describes the landscape of existing services. Factors and areas of interest are identified that are relevant for the adoption of electronic data safes in e-government and e-business using the Unified Theory of Acceptance and Use of Technology as a theoretical lens.
Methodology	This is an empirical paper using an exploratory research approach. Data sources are literature and document analyses, and qualitative interviews with experts based on a semi-structured interview guide. Sense-making was performed by compiling an intermediary report.

Contribution	In the paper, the model of hierarchical service layers is introduced which is assumed to be applicable in other contexts where data management and data processing are decoupled. Factors and areas of interest which might serve as facilitators or barriers for the adoption of electronic data safes are identified.
Co-author's contribution	The article was co-authored by Prof. Dr. Gerhard Schwabe. He commented on the various drafts, revised the paper, and approved the final submission to the conference's reviewing process.

Table 2: Summary of Essay 1's foundational publication

Citation	Pfister, Joachim; Schwabe, Gerhard (2016): „Going Paperless with Electronic Data Safes: Information Ecology Fit and Challenges“. In: Proceedings of the Thirty Seventh International Conference on Information Systems. December 11 – December 14 2016. Dublin, Ireland.
VHB Ranking	VHB-JQ: A
Type of Paper	Research paper
Aim	In this paper, the authors analyze how an electronic data safe fits into an individual's information ecology.
Methodology	This is an empirical paper based on qualitative interviews with 39 participants using thematic analysis as a research methodology.
Contribution	The authors develop a typology of the content that is kept safe in an EDS, reflect upon the motivations and upon an EDS's role with respect to other cloud-based storage services individuals are using. The challenges of maintaining a digital, personal archive are depicted and "data value zones" are introduced as a sensitizing concept to reflect upon problematic areas.
Co-author's contribution	The article was co-authored by Prof. Dr. Gerhard Schwabe. He commented on drafts, revised the paper, and approved the final submission to the conference's reviewing process.

Table 3: Summary of Essay 2's foundational publication

Citation	Pfister, Joachim (2017): "'This will cause a lot of work.' – Coping with Transferring Files and Passwords as Part of a Personal Digital Legacy". In: Proceedings of 20th ACM Conference on Computer-Supported Cooperative Work and Social Computing. February 25-March 1 2017. Portland, Oregon, United States. DOI: 10.1145/2998181.2998262. In press.
VHB Ranking	VHB-JQ: B / A (if acceptance rate < 30%)
Type of Paper	Research paper
Aim	The participants in an interview study describe their current practices and concerns with shaping a digital legacy, especially when they are using cloud-based storage services that unify secure file storage and password management functionalities in one service (electronic data safes). The author reports on the users' coping strategies with respect to shaping and giving access to their digital legacy.
Methodology	This is an empirical paper based on qualitative interviews with 39 participants using thematic analysis as a research methodology. The transactional model of stress and coping (TMSC) is used as an analytical lens.
Contribution	Pre-mortem password sharing is identified as a common problem-focused coping strategy. Moreover, emotion-focused strategies of avoidance and ignorance are discussed. The paper suggests a well-established theory (TMSC) to explain behavior described by benign neglect. Further challenges are described and discussed to, finally, develop design implications.

Table 4: Summary of Essay 3's foundational publication

Citation	Pfister, Joachim and Schwabe, Gerhard (2015): „Electronic Data Safes as an Infrastructure for Transformational Government? A Case Study". In: Tambouris, Efthimios; Janssen, Marijn; Scholl, Hans Jochen; Wimmer, Maria; Tarabanis, Konstantinos; Gascó, Mila; Klievink, Bram; Lindgren, Ida; Parycek, Peter (Eds.) Electronic Government, 14th IFIP WG 8.5 International Conference, EGOV 2015. Thessaloniki, Greece. Proceedings. Springer International Publishing, Cham. pp. 246–257, DOI: 10.1007/978-3-319-22479-4_19.
VHB Ranking	VHB-JQ: not listed Ranked as one of the top conference in the e-government domain (Scholl and Dwivedi 2014).
Type of Paper	Research paper
Aim	The aim of this paper is to identify challenges for solutions supporting transformational government that follow the paradigm of user-managed access based on a user study with ordinary citizens.
Methodology	This is an empirical paper which is based on an exploratory user study involving twelve citizens and three representatives of public and private sector organizations (police, insurance company and a security company) and their interactions with a prototype of an electronic data safe.
Contribution	Four barriers for the adoption of an AEDS in the light of transformational government are discovered: (1.) offering citizens unfamiliar services having the character of experience-goods; (2.) failing to fulfil common service expectations of the customers; (3.) failing to establish contextual integrity for data sharing,

	and, (4.) failing to establish and run an AEDS as a multi-sided platform providing an attractive business model.
Co-author's contribution	The article was co-authored by Prof. Dr. Gerhard Schwabe. He commented on the drafts, revised the paper, and approved the final submission to the conference's reviewing process.

Table 5: Summary of Essay 4's foundational publication

1.8 Contributions to Research and Practice

With its four essays, this thesis contributes new knowledge to answer the overarching research question *RQ0: How can we reduce or even overcome information fragmentation in the context of e-business or e-government processes?* if an (active) electronic data safe is used as a technological solution.

First, practitioners in the field of e-business and e-government can assess what the instantiation of the concept of an electronic data safe would really entail for individuals as end users. This happens on an abstract level related to the suitability of the EDS concept as a whole (essay one) and on a more detail-oriented level with specific usage-scenarios that contributed to uncover new potential benefits, challenges and problems (essay four). Furthermore, the typology of contents and the motivations why people store specific information items in an EDS can be helpful for designing future services and/or functionalities to support the management of these highly-valued information items (essay two). Moreover, the uncovered practices of password sharing are discussed as challenges alongside with possible design implications (essay three). The findings of the third essay are transferrable to any cloud-based information management services when information items will eventually become a digital legacy. In sum, all the findings from the research essays contribute to

answer research question *RQ2: How can we support the exchange of information items via electronic data safes in order to reduce or even overcome information fragmentation?*

Second, this thesis contributes to research by offering an in-depth study of PIM strategies in a multi-device and multi-service world. If an electronic data safe is used, an adequate information ecology fit will be crucial for the adoption but new problems and challenges might arise if the diagnosed "data value zones" (essay two) are (in)voluntarily violated. This concept of "data value zones" extends existing research on PIM and contributes to Human-Computer Interaction research and to the emerging strands on consumer-oriented, behavioral research in Information Systems research. As a second theoretical contribution, PIM strategies are hypothesized to become explainable by referring to a well-established model (transactional model of stress and coping). Thus, the mechanism behind the highly-cited description of "benign neglect" in the domain of personal archiving and PIM is now potentially rooted in theory which might be successfully used to design implications based on this theoretical understanding (essay three). All these findings contribute to answer research question *RQ1: What is the nature of the practices that people exhibit in order to manage information items related to their personal, administrative life?*

2 The Landscape of Electronic Data Safes (Essay 1)

This essay is based on the following peer-review conference paper and has been updated and extended[1]:

Pfister, Joachim and Schwabe, Gerhard (2013): „The Landscape of Electronic Data Safes and Their Adoption in E-Government and E-Business". In: Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS). January 7 – January 10 2013. Wailea, Maui, Hawaii., United States. 1963–1972, DOI: 10.1109/HICSS.2013.532.

Abstract

This essay reports on the concept of electronic data safes for managing personal data and describes the landscape of existing services. Using an exploratory research approach, a model of hierarchical service layers is developed. It serves as a structure for orientation in this emerging field of tools and services. Additionally, perform an in-depth analysis of the business models of electronic data safes using the service business model canvas as an underlying tool. Furthermore, we identify factors and areas of interest that are relevant for the adoption of electronic data safes in e-government and e-business using the Unified Theory of Acceptance and Use of Technology as a theoretical lens. We conclude that clearly perceivable benefits are key facilitators for the adoption of electronic data safes by end-users.

[1] The essay was updated reflecting the changes due to companies entering or leaving this market segment (see footnote 3 on page 38 for details). Furthermore, substantial content has been added in relation to the analysis of an EDS' business models (chapter 2.4) which has also been integrated into the discussion.

2.1 Introduction

Personal data is managed in as manifold ways as there are types of personal data (World Economic Forum 2011). Many tools have been created to assist individuals in their data and (personal) information management – either paper based or electronically (Jones and Teevan 2007a). People connect more and more via social networks and provide personal data on a volunteered basis, or interaction as well as purchase data is tracked and collected by e-commerce companies. But tools supporting user-centric data management and providing users with means to execute informational self-determination to enforce privacy are still in their infancy and about to emerge (Mydex 2009). We subsume all existing solutions and concepts under the umbrella term "electronic data safes". Such technological tools form part of a complex socio-technical system between individuals, service providers (public or private sector) and data safe providers.

Especially in the context of e-government and e-business service provision, these electronic data safes are expected to bring value to each user (individuals or organizations) (Breitenstrom et al. 2008): For example, savings can be realized from optimized processes; data and documents can be exchanged that are accompanied by verified identity data, or transactions involving several (governmental) organizations will be facilitated. We argue, that electronic data safes (see chapter 1.6.4 for an introduction) will provide benefits to all user groups which could not be achieved if organizations stick to their information and process silos like organization-specific portals where users have to re-enter their personal data every time.

Two research questions are addressed: (1.) How can adequate structures be provided for discussing the emerging topic of electronic data safes? (2.) How can factors and areas of interest contributing to the adoption of electronic data safes be identified? In order to answer the first question, we will sharpen the concept of electronic data safes with a focus on e-government and e-business. As a result of our exploratory research, we

(a) provide sensitizing concepts on how to talk about the emerging topic of electronic data safes, (b) analyze business models of existing EDS, and (c) present a model of hierarchical service layers which helps to give structure to the landscape of electronic data safe solutions. To answer the second research question, we attributed our model of hierarchical service layers with dimensions influenced by the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003) as a theoretical lens. Taking such a perspective, we are able to identify factors and areas of interest contributing to the adoption of electronic data safes. By relating the findings from the business model analysis and putting them into context with the findings of the model of hierarchical service layer, we do also point at areas for future design challenges that need to be addressed if EDS adoption and long-term business success shall be achieved.

2.2 What is "Personal Data"?

According to Kuneva (Kuneva 2009), "Personal data is the new oil of the Internet and the new currency of the digital world." This citation illustrates the growing importance and value of personal data (World Economic Forum 2012). But what is personal data?

The European Union defined "personal data" in its Directive 95/46/EC in 1995 as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[2] We are taking a broader perspective informed by Personal Information Management (PIM) and argue that personal data are personalized *information items* which are defined, with respect to PIM, as packages of information that can be created, copied, stored, and retrieved etc. (e.g., digital photographs, music or references) (Jones 2012). This very broad definition of information

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

items reflects the many different forms (paper-based documents, web-based information, structured or semi-structured information items) that people encounter when they are interacting with other people or organizations. This transcends a document or file-based understanding of PIM because information items can be anything, for example entries in digital calendaring tools, digitally managed contacts using a smartphone or information items needed to carry out financial transactions online. We therefore classify personal information items in three groups that are forming a personal "information ecosystem". This classification is based on the latest works discussed at the World Economic Forum (World Economic Forum 2014) which reflect in their evolution (Khatibloo 2011; World Economic Forum 2011) the ongoing discussion how to define a framework of personal data. Three main groups can be identified:

(1.) *Individually provided information:* Such information items are revealed by individual themselves. They can either be "about me", for example, the social security number or user credentials. Or, they can be more "by me", for example, purposefully created as user-generated content. In social networks, such individually provided information items also include, for example, all group memberships, associations and "like"-comments.

(2.) *Observed information items:* All of these information items can be obtained through recording user behavior or observing customers while they are using a service. For instance, this can be location data from mobile phones or Internet browsing preferences. The more data is generated in the future, for example by the Internet of Things, the more relevant it will become how aware the users are of implicit and explicit data collection.

(3.) *Inferred information items:* This type of information items is created and derived by analyzing the behavioral data or voluntarily provided data and combining it with other, existing data sources the individual is not necessarily aware of. These resulting information items, such as the credit card score, are often used for predictive purposes.

This personal "information item" ecosystem is threatened by an imbalance between its three stakeholders: individuals, the public sector, and the private sector. If the private sector dominates, it is very likely that an almost uncontrolled data collection takes place which would deter end-users. If the public sector dominated with too rigid regulations, e.g. data protection laws, innovations and investments could slow down or even be prevented. This fairly new perspective on government as a beneficial regulator is about to evolve but in former times, government was regarded as being the "big brother" who wants keep his citizens under tight surveillance. If the end-users are let alone to self-regulation, islands of working solutions could establish (like Wikipedia) but much insecurity concerning the funding of services or the lack of governance could persist. Therefore, the ideal is to create a "win-win-win"-situation. (World Economic Forum 2011)

Managing the personal information item ecosystem raises questions around privacy (Nissenbaum 2010). Internet users might use services on the web for free, but actually, they pay by providing personal information which can be aggregated to form profiles. In the sense of privacy, users should ideally know what information items they will exhibit and why. To enforce privacy, regulations as well as technological tools can be employed. Both will help individuals manage and control their personal information items, leading to a "New Deal on Data" (Pentland 2009) giving people back the ownership of their data: First, they should have the right to *possess* their own data and companies should act in the role of a trustee or bank of the user's data. Second, they should have full control about the *use* of their data. And third, they should have the right to dispose or distribute their data for whatever reason they like. To achieve this, *informed consent* is the key-mechanism: "Whilst in earlier times control over personal data may have been best undertaken by preventing the data from being disclosed, in an internet enabled society it is increasingly important to understand how disclosed data is being used and reused and what can be done to control this further use and reuse. Consent to the processing of personal data is probably the most important mechanism that currently exists for determining how and when this data can be

used." (Whitley, Edgar A. 2009, p. 155f.). Privacy-enhancing tools (e.g. offering encryption, digital pseudonyms or anonymous payment methods) and transparency-enhancing tools like Google's Dashboard (https://www.google.com/dashboard) to inform an individual which personal information items are stored and why, are helpful technologies in order to exert privacy (Fischer-Hübner et al. 2011).

2.3 Data Collection and Research Method

We followed an exploratory research approach, applying qualitative methods (Myers 1997) such as literature analysis (Levy and Ellis 2006), guided interviews, and evaluation of existing data safe solutions as described in the following chapters. We argue that using this triangulation approach (cf. Kaplan and Maxwell 2005) is an adequate way of data collection for emerging topics. First of all, the data sources we used are depicted. Then, we describe our sense-making approach that took place in order to create the model of hierarchical service layers and to identify factors for the adoption of electronic data safes.

2.3.1 Literature and Document Analysis

Domains, in which the concepts of electronic data safes emerge, were identified as: vendor relationship management (see chapter 1.6.4.4), cloud storage, and managing privacy for personal data. Furthermore, related areas were identified: electronic identity management systems (eIDMS), (personal) electronic health records management systems, electronic document delivery systems via digital postal services or e-billing and e-invoicing services. Additionally, a literature search using scientific literature databases (ACM, Scopus, IEEE, Citeseer, AISeL, GoogleScholar) as well as international union catalogues of library systems, and social bookmarking and citation sharing services was carried out. Literature specific to electronic data safes and the management of privacy with the help of technological tools was found to be very scarce. As an emerging topic that touches many related areas, there are some similar domains and concepts, but no unifying taxonomy exists which helps to

give orientation. The following sources[3] were used (the figures in brackets indicate the number of sources we have consulted), and, where possible, existing public (beta) services of electronic data safes (#7) or cloud storage services (#5) were accessed to gain hands-on experience. Publicly available descriptions, either self-issued by these service providers or written about them by other organizations were also included. These materials consisted mainly of: web pages (#55), journal articles (#52) white papers and reports (#49), research papers and studies (#42), press clippings (#23), blog entries (#13), books or dissertations (#13), other documents (#13) or publicly available annual reports (#2).

2.3.2 Analysis of Existing Data Safe Solutions

We analyzed the following existing electronic data safe solutions, either by gaining hands-on experience with public (beta) services or through the information provided on the web sites and/or personal interviews (see also next chapter). The serviced are grouped as follows:

[3] These sources were initially consulted between February 2012 and April 2012 while writing the internal research report. They were reconsidered and updated in the course of writing the conference paper in June 2012 and on occasion of preparing the camera-ready version in September 2012. Newer versions, for instance, of publicly available annual reports and web pages have also been revisited in order to integrate major developments in this essay until the 20th of December 2016. In detail, for preparing the essay, all the web pages have been revisited and a web search using the search terms "electronic post box", "electronic data safe", "electronic document delivery", "document/data vault/locker" was performed using Google and Google Scholar to identify new sources. Thereby, new services were identified to be researched and integrated as sources for updating this essay. This was the case for Swisscom's Docsafe due to its public launch in June 2014, its branding as a dedicated document safe, and its relatively large user base according to personal communications with Swisscom representatives. Other services have been omitted for a thorough inspection due to their restricted public availability, lack of public accessible information or publications and unclear future prospects. This was the case for the Swiss service "PEAX" (http://www.peax.ch, see next footnote for details) which started as a research project and underwent a transitional phase for a market (re-)launch as a company leading to a phase of instability about the future prospects of this service which coincided with the need to plan research activities for this PhD thesis.

- general purpose file storage/EDS solutions (SecureSafe, and new in 2015: Docsafe), see Table 6;
- electronic data safe solutions originating from the e-government domain (e-Boks, [mein] Service-BW, Dokumentenablage DE-Mail, e-Bürgersafe, e-Tresor), see Table 7;
- process portals in the e-government domain (doMap), see Table 8;
- solutions for aggregating digital documents delivery and electronic bill presentment and payment[4] (Adminium, Zumbox, Doxo, Manilla, Volly), see Table 9;
- solutions for privacy management with a focus on vendor relationship management (Mydex, Pidder, Personal, Trustfabric, Qiy, Azigo, Singly, Allow), see Table 10.

[4] In Switzerland, another service called "PEAX" exists. It serves as an aggregator for documents which are either sent directly and electronically to the PEAX portal or by scanning physically mailed documents. PEAX originated as a research project and it was funded in a public-private partnership (KTI/CTI) at the University of Applied Sciences in Lucerne starting in 2012. No publicly available sources or publications were identified originating from this research project which was transferred into a company in 2014. From this time on, the company reworked its service entirely to launch PEAX 2.0 in July 2016 (https://blog.hslu.ch/crealab/2016/10/07/peax-crealab-forschungsprojekt). In this remodeling phase, the service's status and its future prospects were unclear which lead to the decision to not engage in further investigations and research activities in the course of updating this essay.

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: general-purpose EDS	
SecureSafe[5] Internet-based data safe solution developed by DSwiss and launched in 2008. Besides storing files and being able to share them, a password safe and services to pass on data as a digital legacy are offered, too.	This service still exists. A syncing-client for local file and folder synchronization has been added. Electronic document delivery from trusted senders to the customers, for example, by a bank, has been added, too.
Docsafe Not included in the initial analysis based on data elaborated in 2012.	In November 2013, Docsafe was launched by Swisscom as a safe storage location for all important documents and passwords. Information items can be organized in folders/by tags and they can be shared with other Docsafe users.

Table 6: Solutions serving as general-purpose EDS

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: EDS solutions originating from the e-government context	
e-Boks[6] Danish portal for electronic document delivery. Its mission is to offer companies, public authorities and private individuals a platform for "[...] digital dialogue, and the distribution and storage of important documents." (e-Boks 2016a)	This service still exists. The company running e-Boks has expanded its activities from Denmark to Norway (2012) and Sweden (2015) now reaching 11 million users in the Nordic countries. (e-Boks 2016b) Digital communication G2B/C with mandatory usage has been enforced in 2014 (for a thorough review of the history of this strategy and its effects, see Berger 2015).

[5] http://www.securesafe.com

[6] http://www.e-boks.dk

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: EDS solutions originating from the e-government context	
(mein) Service-BW[7] The portal of the state of Baden-Wuerttemberg in Germany was launched in 2003. In the future, this portal shall open up the vast majority of e-government services to citizens, companies and associations. There is an inbox, an outbox, and a directory for governmental services and responsibilities which will eventually show a link to an electronic service – if it is available.	This service was relaunched in 2015 based on a new architecture and user interface. The document safe component still exists but other components to achieve a citizen portal have been added (electronic ID component). However, the data safe component is not extensively used in the e-government processes offered to citizens, yet.
Dokumentenablage De-Safe[8] Document safe as part of the De-Mail infrastructure in Germany. After piloting De-Mail in Friedrichshafen from October 2009 until March 2010, the accredited providers offered their services to the public in late 2012.	Declared as an optional component in the German De-Mail Law (§8 De-Mail Gesetz), the four accredited De-Mail services have not yet provided services targeting this document safe component. (For more information about the accredited service providers, see Bundesamt für Sicherheit in der Informationstechnik 2016)
eBürgersafe[9] An application to demonstrate the usefulness of the electronic identity management system's functionality of the new German identity card, piloted in the state of Bremen and the city of Bremerhaven, Germany.	This service is not online any more. No information could be found what happened to it.

[7] http://www.service-bw.de

[8] http://www.de-mail.de

[9] In 2012, it was reachable via http://www.buergersafe.bremen.de

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: EDS solutions originating from the e-government context	
e-Tresor [10] Electronic safe for storing documents and receiving documents supported by an eIDMS component.	In 2012, this service was a marketed as a standalone-service. In 2015, it has been integrated into the Austrian e-ID solution of the "Handy-Signaturkonto" and the data safe component is used as the inbox and outbox for documents signed with the Austrian eID. Nevertheless, it can be also used to store own documents but it is now seen more as a secondary component for the leading eID solution. Additionally, users can create and digitally sign invoices.

Table 7: EDS solutions originating from the e-government context

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Process portals in the e-government domain	
doMap[11] Process-oriented portal of the city of Dortmund, Germany offering electronic postal box and e-government processes with e-payment. The portal was launched in 2002 (Stadt Dortmund 2004) and a separation between front-office and back-office tasks is performed (Meyer-Jäkel 2011)	This service still exists.

Table 8: Process portals in the e-government domain

[10] http://www.e-tresor.at

[11] http://www.domap.de

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Solutions for aggregating digital documents delivery and electronic bill presentment and payment	
Volly[12] Pitney Bowes, a company well-established in the conventional mail industry, created Volly as a product that aggregates electronic bills from several senders and offers targeted communications and commercials which have been opted-in by the end-users. ("It's a secure, spam-free, opt-in digital delivery service that will empower consumers to receive, view, organize and manage all household account statements, and more, including online bill pay from the multiple companies they do business with.", FAQs from Volly in 2010). The launch for the US market was announced in 2011.	Volley has not been launched as a stand-alone product for end consumers. Pitney Bowes seemed to have substantial problems to push that solution with the document senders. That is why they performed a massive strategic shift and re-branded Volly now called "Inlet" alongside a new joint venture with the company Broadridge Financial Solutions to redesign the service. Initially, Volly had been targeted as a front-end to the end-customers hiding the document senders. Inlet is now more of a platform running in the background. It is able to be integrated in the document provider's portals that are facing to the end-customer. Furthermore, e-payment options are given and marketed as a value proposition of the new Inlet platform (Stein 2014). According to Inlet, 3000 financial institutions and bill payment sites are connected with possibly 200 million consumers.

[12] In 2012 reachable via http://www.volly.com, now it is www.inletdigital.com

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Solutions for aggregating digital documents delivery and electronic bill presentment and payment	
Adminium[13] Digital filing system to aggregate bills and invoices from several senders to avoid that the users have to check many portals separately. The service was started October 20, 2010.	This service went out of business in Autumn 2013. The company was deregistered in October 2013. No information was found why this happened.
Zumbox[14] This service offered a digital mailbox to accept documents only from trusted senders thereby aggregating document reception for the end-users. It was marketed as a hybrid mail service launched in October 1st, 2006 as a digital enrichment of a physical address.	This service was stopped in April 1st, 2014 because no further investor was available. It was diagnosed that for digitized, transactional mail the time and the cost to deliver the service was more than the market was prepared to invest at that time (McDermott 2016; @niral89 et al. 2016).
Manilla[15] This service was a consolidator for electronic-invoices and went into the market in February 2011. As a customer, you could choose the senders that were allowed to send documents and invoices to you which could be paid via Manilla using its e-payment services.	The company closed in July 2014. It was diagnosed that they did not achieve the scale which had been necessary for a sustainable business (Ha 2014; @niral89 et al. 2016).

[13] In 2012, it was reachable via http://www.adminium.fr

[14] In 2012, it was reachable via http://www.zumbox.com

[15] In 2012 reachable via http://www.manilla.com

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Solutions for aggregating digital documents delivery and electronic bill presentment and payment	
Doxo[16] This service started in May 2010 and was marketed as a digital filing cabinet which is accessible from everywhere and reduces the need for paper. Users can connect with businesses. A password safe was available and bills could be payed via an e-payment component.	This service is still available. They re-focused on the electronic bill payment as the primary value proposition. The former focus being a digital filing cabinet has disappeared.

Table 9: Solutions for aggregating digital documents delivery and electronic bill presentment and payment

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Solutions for privacy management with a focus on VRM	
Mydex[17] Mydex is registered as a community interest company aiming not for profit maximization but to contribute to a social purpose. The company intends to educate individuals about the value their personal data has and to provide them the technological toolset to empower citizens by exercising control over their personal data. Therefore, they adopted the VRM perspective and created Mydex as a personal data store. (Heath et al. 2013)	The company is still in business. Nevertheless, it seems that no public available product has been launched to date.

[16] http://www.doxo.com

[17] http://www.mydex.org

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Solutions for privacy management with a focus on VRM	
Personal[18] In 2012, Personal.com marketed its service as a personal data store with respect to the VRM concept. Personal data was regarded as goods that has a value in exchange and the service of personal.com helps individuals to control this. Information items were stored as "gems" and could be shared. (Tanner 2014)	The company rebranded itself to teamdata.com and refocused their business activity to manage information items for teams. The VRM ideas has been dropped entirely.
Qiy[19] The vision of Qiy (spoken: "key") is to help individuals re-gaining control over their fragmented information items while creating value for organizations (Rudland 2012). At the time of the initial research in 2012, access to QIY was only provided on invitation. The QIY platform was licensed by the Qiy foundation.	The Qiy company was renamed to Digital Me BV. A Proof of concept following the initial vision of Qiy was implemented. Furthermore, a "minimal viable product" was developed serving as a showcase. The Qiy foundation is also still operational.
Azigo[20] Azigo aimed at aggregating communications from several e-commerce providers for consumers to offer a "lifestream for consumers". By bundling loyalty programs, e-commerce accounts, and marketing mails, users should be able to manage which organization should be allowed to send offers to them. Profile data should be reused on a user-managed access paradigm to avoid manual retyping.	The service still exists. For the customers, it serves as hub unifying several mailings from vendors at one single point. Furthermore, they are incentivized to earn points for further reductions/cash backs. A number of 9000 active users in 2015 has been reported (https://angel.co/azigo).

[18] In 2012 reachable via http://www.personal.com

[19] http://www.qiy.nl

[20] http://www.azigo.com

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Solutions for privacy management with a focus on VRM	
Pidder[21] Pidder (Private IDentities Demand Encrypted Resources) was a personal data store following the Privacy-By-Design concept. Each individual decides which information items should be disclosed to which other party or group using a fine-grained authorization mechanism. Information items were stored as information cards, grouped into wallets and providing multiple identities and personas. Pidder was developed by Versaneo GmbH founded in 2008.	The company developing Pidder was liquidated in January 2016. No information was found how successful the product had been or why the company ceased its existence.
TrustFabric[22] This company intended to support trusted communications between individuals and companies. Therefore, an individual could select for each organization which channels should be used to communicate. A data safe was also integrated where files could be shared. The company was founded in 2010.	The company does not exist anymore and no further information could be found what happened to it.
Singly[23] The initial aim of Singly was to give an individual back control of its own, personal data. Unifying the distributed information fragments in one single location was the intended approach, thereby creating a marketplace and a platform. The company was founded in 2011 but no demo version of its software has been provided then.	The company was bought by Appcelerator in 2013 in order to exploit their experience in API extraction – not the initial service to control personal data.

[21] In 2012 reachable via http://www.pidder.com

[22] In 2012 reachable via http://www.trustfabric.com

[23] In 2012 reachable via http://www.singly.com

service name and description based upon first encounter in 2012	changes occurred between 2012 to 2016
Category: Solutions for privacy management with a focus on VRM	
Allow[24] Initially, the company aimed with its service for private customers to give them back control about their own data with respect to marketing activities by companies. In their Allow account, users should select which companies are allowed to send marketing materials to them based on a profile of self-identified interests. No real background information on the company behind Allow was found in 2012.	The company and the service itself of Allow have vanished after February 2013 when the last official Tweet had been sent (@iallow).

Table 10: Solutions for privacy management with a focus on VRM

An EDS can also be analyzed by interpreting it as a platform. Parker et al. (2016) define a platform as *"[…] a business based on enabling value-creating interactions between external producers and consumers. The platform provides an open, participative infrastructure for these interactions and sets governance conditions for them. The platform's overarching purpose: to consummate matches among users and facilitate the exchange of goods, services, or social currency, thereby enabling value creation for all participants." (Parker et al. 2016, p. 5)* In their work, these authors also introduce the notion of different roles leading to different models for managing and sponsoring platforms. They discern between the roles of (a) the platform manager and the platform sponsor, (b) the roles of the developers (core, extension and data aggregators), and (c) decisions regarding the amount of user participation and their roles. Albeit not all analyzed EDS solutions are already platforms, many EDS services suggest having a potential to become a platform in the future – or they have initially shown this tendency but then re-branded themselves. Therefore,

[24] In 2012 reachable via http://www.i-allow.com

we report on the analyzed EDS solutions and their platform-readiness by describing their business organization and the stakeholders involved. The results are described in Table 11 and Table 12.

	Platform Manager	
Platform Operations		**SecureSafe**
DSwiss AG	DSwiss AG	**Docsafe**
Swisscom AG	Swisscom AG	**e-Boks**
KMD Ltd. (developing IT solutions and hosting for Danish municipalities)	e-Boks A/S	**Service-BW**
BITBW (Landesoberbehörde IT Baden-Württemberg as a division of the Department of the Interior)	Department of the Interior of the State of Baden-Württemberg	**Dokumenten-ablage DE-Mail**
DE-Mail Service Provider	Each DE-Mail Service Provider following the standards require in the DE-Mail law	**e-Bürgersafe**
Governikus GmbH & Co. KG	Governikus GmbH & Co. KG	**eTresor**
A-Trust GmbH	A-Trust GmbH	

Extension Developer	Core Developer	Platform Sponsor	
Closed model	DSwiss AG	DSwiss AG (indirectly: venture capital firms funding DSwiss)	**SecureSafe**
Closed model	Swisscom AG	Swisscom AG	**Docsafe**
Closed model	e-Boks A/S	e-Boks company (50% Nets and 50% Post-Nord) and the Danish Government mandating/regulating e-Boks usage.	**e-Boks**
Closed model	Seitenbau GmbH on behalf of the Department of the Interior of the State of Baden-Württemberg	Department of the Interior of the State of Baden-Württemberg	**Service-BW**
Closed model	DE-Mail Service Provider	DE-Mail Service Provider	**Dokumenten–ablage DE-Mail**
Closed model	Governikus GmbH & Co. KG	State of Bremen	**e-Bürgersafe**
Closed model	A-Trust GmbH	Austrian Federal Chancellery	**eTresor**

	Users	Data Aggregators
SecureSafe	• Private individuals • Business customers	Closed model
Docsafe	• Private individuals • Business customers	Closed model
e-Boks	• Private individuals • Business customers • E-Government divisions	Closed model
Service-BW	• Private individuals • Business customers • E-Government divisions	Closed model
Dokumenten-ablage DE-Mail	• Private individuals • Business customers	Closed model
e-Bürgersafe	• Private individuals	Closed model
eTresor	• Private individuals • Business customers	Closed model

Table 11: Roles and responsibilities, part 1

Platform Operations	Platform Manager	
Dortmunder Systemhaus (dosys)	City of Dortmund	**doMap**
The startup-company itself when it was still existing.	The startup-company itself when it was still existing.	**Adminium/ Zumbox/Manilla**
Doxo Inc.	Doxo Inc.	**Doxo**
Inlet using Amazon Web Services	Inlet LLC (Pitney Bowes 50% and Broadridge Financial Solut. 50%)	**Volly/ (now: Inlet)**
Personal Inc.	Personal Inc.	**Personal/ (now.) Teamdata**
Mydex CIC	Mydex Cummunity Interest Company (CIC)	**Mydex**
Individual company, using licensed schema from Qiy fdt.	Qiy Foundation	**Qiy**
Azigo Inc.	Azigo Inc.	**Azigo**

Extension Developer	Core Developer	Platform Sponsor	
Closed model	Dortmunder Systemhaus (dosys)	City of Dortmund	**doMap**
Closed model	The startup-company itself when it was still existing.	The startup-company itself and venture capital firms backing them.	**Adminium/ Zumbox/Manilla**
Closed model	Doxo Inc.	Doxo Inc. (and the venture capital firms backing this company)	**Doxo**
Potentially open	Inlet LLC	Pitney Bowes 50% and Broadridge Financial Solutions 50%	**Volly/ (now: Inlet)**
Closed model	Personal Inc.	Personal Inc. (and the venture capital firms backing this company)	**Personal/ (now.) Teamdata**
Closed model	Mydex CIC	Mydex CIC (open for investors respecting the legal embodiment as a CIC)	**Mydex**
Open by licensing	Qiy foundation / Digital Me BV	Qiy foundation	**Qiy**
Closed model	Azigo Inc.	Azigo Inc. (and the venture capital firms backing this company)	**Azigo**

	Users	Data Aggregators
doMap	• Private individuals • Business customers • E-Government divisions	Closed model
Adminium/ Zumbox/Manilla	• Private individuals • Business customers	Closed model
Doxo	• Private individuals • Business customers	Closed model
Volly/ (now: Inlet)	• Private individuals • Business customers	Potentially open
Personal/ (now.) Teamdata	• Business customers	Closed model
Mydex	• Private individuals • Business customers • E-Government divisions	Closed model
Qiy	• Private individuals • Business customers	Closed model
Azigo	• Private individuals • Business customers	Closed model

Table 12: Roles and responsibilities, part 2

2.3.3 Qualitative Interviews

We further carried out seven interviews with stake-holders in the realm of electronic data safes each lasting about 90 minutes. The stakeholders were mainly representatives of organizations running an electronic data safe or people involved in designing such solutions, and academics doing research in this area. For all these interviews, a questionnaire had been prepared as a basis for each guided interview which was audio-recorded.

The design of the initial questionnaire was informed by literature on electronic data safes (notably Breitenstrom et al. 2008) as well as public accessible information on web pages or by testing existing data safe solutions. Consulting these sources, areas of interest emerged and were refined leading to a questionnaire with several categories. These categories were: a solution's context (stakeholders, history of the service, responsibilities for operating or developing the service, orientation on existing e-

government strategies), design decisions concerning identity and access management, general functionalities of the service (for example, what data sharing mechanism are available), data on a solution's current usage (number of users, number of logins, etc.), its business model, and future directions. Each questionnaire was customized to every stakeholder and refined throughout the course of the data collection phase.

Additionally, two customers of an existing electronic data safe solution were interviewed to capture their views from a client's perspective. These interviews took about 45 minutes each. A questionnaire was used as a basis for the guided interviews. Questions were dealing with individual usage habits like frequency, number of documents stored in their electronic data safe and their attitude towards security and the usability of their data safe's identity and access management from an end-user perspective.

2.3.4 Sense-making

The interview data was then summarized based on the structure of the questionnaires. To verify that nothing has been omitted, the individual reports were checked while re-listening to the audio-recordings. Finally, the reports were complemented with web findings and literature findings on the specific solution and an internal report documenting the state-of-the-art of electronic data safes has been compiled. During the composition of this report, a schema to organize the findings and to group data safe solutions emerged – in the tradition of exploratory research. We then generalized from this data and the model of hierarchical service layers (see chapter 2.4) was created which allowed us to sort data safe solutions according to their maturity and provided structure to the emerging landscape of electronic data safes thereby answering the first research question.

Based on this model of hierarchical service layers, we tried to answer the second research question: How to identify factors and areas of interest contributing to the adoption of electronic data safes? Therefore, we initially attributed our model of hierarchical service layers with dimensions

influenced by the UTAUT as a theoretical lens. UTAUT was chosen because of its widespread use in information systems and its incorporation of prior technology acceptance models resulting in a parsimonious model with four constructs (Venkatesh et al. 2003): *Performance expectancy* is defined as "the degree to which an individual believes that using the system will help him or her to attain gains in job performance." *Effort expectancy* is defined as the "degree of ease associated with the use of the system." *Social influence* is defined as "the degree to which an individual perceives that important others believe he or she should use the new system." *Facilitating conditions* are defined as the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system." Further, UTAUT includes four moderating factors: *gender, age, experience,* and *voluntariness of use*.

The interview reports were analyzed for evidence of UTAUT's constructs and moderating factors. While working through the reports, we discovered that not all UTAUT constructs could be applied: No evidence was found for the constructs of social influence and all the moderating factors. During our sense-making process, we found evidence that other factors influencing the adoption exist: We conclude that electronic data safes are network goods and they will benefit from network effects from both, the end-users, and the organizational users. UTAUT's "social influence" (oriented towards the end-users) can be subsumed under network effects, thereby also paying attention to the network effects which are clearly effective for all organizational users of electronic data safes. Furthermore, we included hedonics (Hassenzahl 2010) as a dimension of analysis which originally is not included in the UTAUTs' constructs. Hedonic aspects originate from user-experience research in which the creation of a holistic user experience incorporating pragmatic qualities as well as hedonic qualities are regarded as necessary to design an appealing, interactive product. The pragmatic qualities help to achieve "do-goals", such as "making a telephone call" where functionalities and usability are decisive. In contrast, hedonic qualities support "be-goals" which give the reason why people are making a telephone call, such as the desire to relate to one's significant other (Diefenbach and Hassenzahl 2011).

2.4 An Analysis of Business Models for EDS

By analyzing business models, different approaches for value-creation and value-capturing can be identified and compared. Osterwalder (2004, p. 15) defines a business model as follows*: "A business model is a conceptual tool that contains a set of elements and their relationships and allows expressing a company's logic of earning money. It is a description of the value a company offers to one or several segments of customers and the architecture of the firm and its network of partners for creating, marketing and delivering this value and relationship capital, in order to generate profitable and sustainable revenue streams."*

In his work, Osterwalder suggests nine dimensions, the "business model ontology", that characterize a business model. These dimensions are the foundational components of the widely-used "business model canvas" (BMC; Osterwalder and Pigneur 2010) which serves as a visualization of the key elements of a business model and how they are related. Nevertheless, the BMC has a company-centric view towards its business activities following a traditional one-sided business logic. There is an ongoing trend that recognizes value creation as an activity of value co-creation between customers and companies following the paradigm of the service dominant logic (Vargo et al. 2008; Vargo and Lusch 2004) and service logic (Grönroos 2008, 2011). According to Vargo and Lusch (2008, p. 26), *"[...] service is defined as the application of specialized competences (operant resources—knowledge and skills), through deeds, processes, and performances for the benefit of another entity or the entity itself."* These considerations motivated Zolnowski (2015) to combine service-orientation with the analysis of business models resulting in a "Service Business Model Canvas" (SBMC) (Zolnowski et al. 2014; Zolnowski and Böhmann 2011, 2014). The SBMC takes the dimensions from the BMC and differentiates between the perspectives of the company, the customer and the partners in order to cover the two-sided or multi-sided nature of service offerings (see Figure 2).

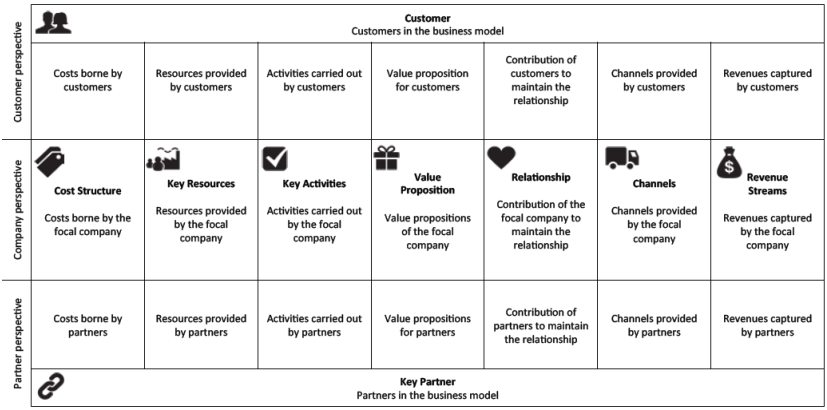

Figure 2: Service Business Model Canvas (Zolnowski 2015, p. 30)

In our understanding, an electronic data safe is a socio-technical system whose value-creation is based on an interwoven set of service offerings (a) from the EDS platform provider (the focal company), (b) the service providers delivering service(s) using the EDS platform, and (c) the customers that are taking part in value co-creation activities by using the EDS. Therefore, a business model analysis for EDS needs to pay attention to the multi-sided nature of all stakeholders involved which is achieved by using the SMBC as a theoretical lens. Such a separation was also suggested in the work of Kemppainen (2016) analyzing data management platforms in the health sector. In the remainder of this chapter, we will report on the findings form our business model analysis using the SMBC for EDS. For our analysis, we focus on the still existing services of the time of the writing of this thesis (December 2016) which are:

- general purpose file storage/EDS solutions (SecureSafe, and newly added in 2015: Docsafe)
- electronic data safe solutions in the e-government domain (e-Boks, Service-BW, eTresor)
- process portals in the e-government domain (doMap)

- solutions for aggregating digital documents delivery and electronic bill presentment and payment (Doxo, Volly, Azigo)
- solutions for privacy management with a focus on vendor relationship management (Mydex, Qiy, Personal/Teamdata)

Each EDS service was analyzed using the SMBC; each of the canvases can be found in the appendix to this essay (chapter 2.8). The results are summarized in the following chapters 2.4.1 - 2.4.9 for each dimension of the SBMC.

2.4.1 Customers

The *customers* of EDS solutions were either private individuals or business customers (such as teams). Especially the EDS solutions within an e-government context had public authorities as stakeholders with divisions using or designing e-government services.

2.4.2 Key Partners

As *key partners*, one would often consider an organization who is running an EDS in the sense of a platform manager to serve as the only stakeholder. But often, there are several groups of stakeholders. For example, if the platform operation is outsourced, the companies responsible for that part are key partners. In the domain of e-government, the authorities itself often draft and fund projects, but the actual implementation and the service's operations (such as hosting) is performed by another company (for example, KMD with e-Boks or Seitenwerk with Service-BW). Moreover, when documents from multiple organizations are delivered with an EDS, these document senders will become key partners because they increase the attractiveness of the EDS service by bringing more value (in form of a reduced information fragmentation) to the individuals using an EDS.

2.4.3 Cost Structure

The *cost structure* of the different EDS services needs to be analyzed according to the stakeholder's perspective.

For *customers* (individuals or legal entities such as businesses), the services are offered predominately for free or follow a freemium pricing model, for example, to obtain a larger amount of storage.

From the perspective of the *focal company*, the cost structure is determined by costs for staff, marketing and business development activities, operations and software development. This is the same for EDS services provided as part of public services or EDS services run by private companies. Business activities such as software development or operations might be outsourced by the focal company which is not always transparent and hard to identify using publicly available, external documents and information. For the public sector, if an EDS is seen as a component in a larger e-government service architecture, the EDS service will be conceptually developed and aligned to the e-government strategy by the public authorities acting as principals. But the actual implementation and operations of an EDS are either outsourced (platform "Service-BW" by the Ministry of the Interior of the State of Baden-Württemberg: Seitenbau GmbH, eTresor: A-Trust GmbH, Agency for Digitisation at the Ministry of Finance in Denmark: e-Boks) or run by internal competence centers (doMap: dosys as the Dortmunder Systemhaus). Albeit an open market exists and public procurement with tenders are performed, public authorities require applicants to possess certifications or accreditations thus creating a temporary monopoly for an outsourcing partner as the partner of choice for a given period of time.

Platform partners having the role of *document senders* are mostly charged with a per document fee (SecureSafe, Docsafe, e-Boks, Volly) and/or one-time or periodic setup or connection fees (Mydex). Another EDS service charges the document provider by demanding a commission for purchases initiated through the platform (Azigo). Based on the public available information, Qiy charges the document providers indirectly by its licensing fees to use the Qiy information exchange metadata scheme.

2.4.4 Key Resources

Having a closer look at the *key resources* of the EDS services under inspection provides us with the following picture:

The *customers* need compatible devices to access the EDS service (computers or mobile devices). If payments shall be executed via the EDS, customers also need an accepted method of payment. And if documents or bills are aggregated by the EDS, a pre-requisite from the customer's or citizen's perspective is that their desired service provider is also connected to the EDS. This connectedness of the service provider can be interpreted implicitly as a key resource for the customers because for them, such a connection is vital to receive benefits by the use of an EDS. Generally, the customers must be willing, to store personal data in the cloud which reflects the problem of trust with cloud-based services in general. Especially, if e-government offerings are involved, other components, such as an electronic identity, are often a pre-requisite to use an EDS (Handy-Signatur for the e-Tresor in Austria; NemID for e-Boks in Denmark). Thereby, these components are re-used, something that also happens in the private sector by re-using established accounts and account credentials (such as the "Swisscom Login" for Docsafe).

From the *focal company's* perspective, common key resources are: staff, software, (server) hardware, and established connections to document providers. Therefore, interfaces (APIs) must be provided in order to deliver documents into the EDS (for example, SecureSafe and Docsafe provide such APIs to connect with a document provider's backend systems). If the service is embedded in an e-government infrastructure (Service-BW, e-Boks, e-Tresor), eID-components are widely used or, in the private sector, existing account credentials are re-used (Docsafe with the "Swisscom Login"). Generally, a trusted and secure way of authentication is actively used by the European EDS service offerings, for example, eID solutions or 2-factor authentication using SMS with a self-registered mobile phone number (SecureSafe). If payment needs to be executed (for the focal company itself or on behalf of document senders/bill provider), widely accepted payment options should be offered in order to automate

billing. The geographic location of the servers, where the information items are stored, is also a key resource that is actively marketed by European EDS services (SecureSafe, Docsafe, e-Tresor, Service-BW) in contrast to a globally distributed storage "somewhere" in the cloud or in countries with less stringent data protection laws. For focal companies, signaling trust is also a key resource that is handled differently (Mydex: legal status of a Community Interest Company; SecureSafe, Docsafe, and e-Tresor: data storage based in the respective home country where the service is domiciled). Other key resources are licenses to use a metadata scheme in order to connect to customers and service providers, such as it is enforced by Qiy. Another key resource is the approval or accreditation by governmental stakeholders if private companies have been selected in public tenders to implement and run the services thus creating a temporary monopoly for this kind of service for a fixed period of time (doMap: Dortmunder Systemhaus; Service-BW 2.0 with the company Seitenbau whereas Service-BW 1.0 and the documents safe therein had been developed by T-Systems). Having an official mandate often goes along with being granted financial support for a defined period. Furthermore, a company's reputation and already established standing – maybe even signaling its disconnectedness with government – might serve as a key resource to promote its EDS service (Docsafe offered by Swisscom, the partly denationalized telecom provider in Switzerland with the largest market share). Other companies in the private sector try to benefit from effects of trust inference based on their collaboration with other trustworthy companies, such as banks, or that the service is "Swiss made" (SecureSafe).

When we have a look at the *platform partner's* key resources, we have to distinguish between (1.) document providers and (2.) contractors for EDS development an/or operations. First, *document providers* need to connect their backend systems to an EDS using APIs. These are key resources for them. Besides, they need to have staff who is able to carry out these connections on a technical and managerial level, maybe also requiring legal expertise related to electronic document delivery. And of

course, document providers need to have benefits from electronic document delivery compared to physical mail delivery, for instance, due to cost reductions. Second, if the EDS provider has *contracted other companies* for the development and/or operations of the EDS service, these contractors need trained staff, software and hardware to perform this task.

2.4.5 Key Activities

Regarding the *key activities* of the different stakeholders, we distilled the following practices:

For the individual *customers*, the key activities are: registration with the EDS service, authenticate as registered user (maybe using 2-factor authentication mechanism), accessing information items, adding information items, possibly carry out or initiate payments, storing information items, sharing information items, and, finally configuring the EDS service to one's own needs. The connections needed in the background to deliver documents or send documents or information items are not visible to the individual, for example, which framework or APIs are needed. If several document senders exist and an active opt-in is necessary, individuals must select document providers during setup or configuration activities. If the EDS service provider offers a loose-coupling with other document providers via a dedicated EDS "e-mail"-address, it is the individual customers' duty to announce it to potential document senders. If the EDS has been mandated by a country's e-government strategy, it is the individual's obligation to check the EDS contents regularly for new and relevant documents.

The EDS platform providers as the *focal companies* execute key activities related to product and service development. They have to manage all outsourced activities (such as billing, operations, development). Furthermore, the EDS platform provider is responsible for integrating and maintaining payment options. If the EDS platform provider is a governmental unit, it has to follow or enforce the given e-government strategies. Albeit support-activities are an essential criterion for successful adoption, the

commercially delivered EDS solutions seem to embrace the idea of supporting their (paying) customers to achieve their goals better than the services with mandatory usage in the e-government domain. There, an EDS is often regarded as "one additional" channel which is not really integrated with existing practices or has been replaced other channels. Another central key activity of an EDS platform provider is the management of the platform participants, notably the acquisition of new partners for document delivery to increase a platform's attractiveness. These acquisition activities might also entail the (pro-)active management of partners and questions related to legal, financial or technological issues.

The key activities with respect to *platform partners* of an EDS need to be discerned between (1.) the document providers and (2.) contractors helping to run the EDS platform. The key activities of the *document providers* are mostly related to document or information item delivery in an EDS. Therefore, they need to use APIs to deliver information items and provide support for automatic billing or payment. Being able to connect to one or several EDS with a platform partner's output management systems is a key activity to keep running the document delivery as part of the partner's operations. If *contractors* are involved for running an EDS operations, their key activities consist in service development or operations and integrating the EDS solution with other components mandated by the principal's e-government strategy, such as an eID.

2.4.6 Value Propositions

Now, we have a closer look at the *value propositions* that are promised by the different EDS services.

From the *customer perspective*, the EDS services promise to make personal information management with respect to officially received documents easier by: uniting and centralizing all important information items at one place, accessing them from everywhere, re-using existing information items for different service-providers, execute payments, and being able to take part in B/G2B/C communication. Furthermore, some

EDS services (especially the European ones) put emphasis on data security; they offer secure and encrypted storage that is located in countries with higher data protection standards. Some other services put their emphasis on the user-managed access paradigm, that means, that they intend to give user's back control about their information items and let them decide who will use them or with whom they will share them. The ubiquitous access for information items in an EDS is marketed as an advantage for the customers and the security mechanisms of a data safe are praised as protective elements due to the service's cloud-based nature. Another value proposition for the customers, especially for the services originating from the e-government domain, is their connection to e-government processes that may be initiated in the EDS service itself or other services given access to information items stored therein. Such EDS service offerings, such as Service-BW, see themselves as the single point of contact for G2B/C or B/C2G interactions. Remarkably, the companies following the VRM paradigm that emphasize user-managed access as the unique value proposition for customers, such as Qiy and Personal (now Teamdata), seem to have had bigger challenges of selling their value proposition to the customers over the years and creating marketable services and products. For example, Personal started with a focus on VRM and re-using and sharing data based on the user-managed access paradigm in an inter-organizational context. By the time, it has redefined its value proposition to help teams share a team member's personal information items using their original technology intended to work in a larger and inter-organizational context – a change, that is also reflected in Personal's rebranding as Teamdata.

The value propositions for the *focal company* are predominately related to visions of becoming a hub or platform for managing personal information items and carrying out transactions. For the commercially oriented EDS services, a pattern emerges: They often aspire to become "the" or "a major player" in the market for managing personal information items by acting as a hub or platform. They recognize that they need to become a platform to achieve attractiveness and contribute to the value-creation for their various stakeholders. That is why the value propositions

of the EDS platform providers do reflect the value propositions given to the customers: unify and centralize document management to have everything important stored in one location with ubiquitous and secure access, give the customers control over their information items by letting them decide with whom they can be shared with or re-used, provide secure paperless billing and bill payment services, improve electronic document delivery in the B/C/G2B/C/G sector by substituting conventional, paper-based mail and postal providers, and emphasize their country of origin as decisive and discerning factor with respect to data protection laws. They strive for establishing an image as a predictable and secure partner that can be entrusted with all the sensitive information items, for example, by collaboration with trustworthy partners, such as banks. The VRM providers, so far, do only focus on the user-managed access mechanisms as their key value-proposition whereas other EDS services, especially in the domain of e-government, go beyond pure data storage by integrating information items into processes and transactions. VRM providers intend(ed) this, too, but they seem to lack viable business or organizational partners to put their vision and value proposition into (commercially successful) practice.

The *platform partners* of an EDS, notably in their role as document providers or recipients of information items, experience a different set of value propositions brought to them by EDS services: electronic document delivery is faster and cheaper, the delivery of documents and transactions take places in a secured environment, they have access to authenticated customer data and authenticated information items, and finally, they do not need to develop an own infrastructure for document delivery or payment and can focus on their key competencies thereby reducing transaction costs for all EDS platform users. By using an EDS, they can position themselves as modern organizations that are connected with their customers using future-oriented channels providing more value to every stakeholder.

2.4.7 Relationship Dimension

In the next paragraphs, we will report on the *relationship dimension* of the SMBC for EDS.

From a *customer's* point of view, the analyzed EDS solutions do favor a customer relationship based on self-service for registration and use. Only Qiy as a foundation tries to form close contractual relationships because the end customers of the Qiy Foundation are organizations. These organization should become a member and then provide services to individuals. The level of closeness with the customers is, as the personal data store Personal/Teamdata demonstrates, tied to the subscribed plan.

The *focal company* as the platform provider fosters its *customer relationships* through automated service delivery. This means, that customers use the functions and processes defined by the platform provider without the need for a customization. Therefore, the EDS platform providers can serve huge numbers of customers with their product following the classical concept of economies of scale. In order to achieve these economy of scale effects, automating most of the interactions and minimizing manual interventions or support issues are design aims of EDS solutions. That entails to have close relationships with *bill providers or document providers* to win them as customers and help them setting up their backend systems to fully automatize bill presentment and payment processes carried out via an EDS.

The *platform partners* exhibit several types of relationships that must have been established administratively via contracts and automated on a technical level: the connected partners need to accept payments made via the specific EDS service or another service provider, they need to support the exchange of information items based on a user-managed access paradigm using defined APIs, and connect their backend systems for document or information item delivery and reception. With respect to the customer relationship, if document providers move to an EDS for sending documents to their customer, they give up their direct visibility for the customers. This is a major challenge for all EDS service providers to

provide mechanisms or design solutions that care for the loss of the formerly more direct supplier-customer relationship which arises from interacting with an organization's specific portal instead of using an aggregated and "neutral" EDS. We assume that this issue was behind Volly's strategic re-orientation to become "inlet" and focusing more on providing backend-services retaining the provider's first face to the customer impression using their portals.

2.4.8 Channels

When we have a look at the *channels* that are used to interact with an EDS, *customers* use either the EDS's website or mobile devices, maybe with EDS specific apps, to administrate their information items. File-based EDS solutions provide synchronization clients or clients that facilitate document or file uploads. The focal companies use mainly the same channels as the customers but for their business partners, such as document suppliers, they also offer APIs to automate the exchange of information items. And the *platform partners* are mostly dependent on connecting their backend systems to an EDS using the provided APIs.

2.4.9 Revenue Streams

Finally, we analyze the *revenue streams* of the EDS services.

For the *customers*, a direct revenue from using an EDS is hardly derivable. Nevertheless, we argue that most individuals as customers will benefit by time savings and less efforts. With respect to Azigo being an exception, customers receive rewards/benefits related to loyalty programs.

The *focal companies* need to attract revenues and different strategies exist. For example, Azigo takes 7.5% commission for purchases initiated via its platform. If documents are delivered, the platform providers usually will charge a document delivery fee, equivalent to a stamp for physical delivery which is paid by the sender. Besides, the platform provider might charge a one-time connection fee or yearly service fees which might also manifest in the form of licensing fees (Qiy). Other services follow a freemium pricing model to attract customers and to bill them for a higher

service level, for example, offering extended storage volume. Customers are then requested to pay a usage fee, mostly on monthly/yearly basis and per user. If the company is big enough, cross financing with other products or services might be performed, especially in the market penetration phase (for example, Swisscom) to overcome the chicken-egg problem how to attract customers and service providers. For the EDS services having their roots in the e-government domain, there are no direct revenues that must be generated because these services are funded by tax money.

The *platform partners* need also to generate revenues and do this mostly by charging their customers for using their services – and thus indirectly paying for using the EDS services. The necessary funding of the EDS as an intermediary might cause active resistance, as it is the case for Doxo: Some companies do not want to pay the commissions that Doxo demands and request their customers to pay using their portals directly. If platform partners are responsible for the operation of the platform, for example by running the data center or developing new functions – something that is common in the e-government domain – then the revenues are based on project funding or longer term contracts with tax money as the ultimate funding resource.

2.5 Model of Hierarchical Service Layers

Narayanan et al. (Narayanan et al. 2012) offer a classification scheme for "personal data architectures". However, they suggested that other classifications might be possible as well. Based on our sense-making approach (see chapter 2.3.4), we propose that there are three hierarchically grouped service layers for electronic data safes: (1.) (cloud) storage services, (2.) value-added services, and (3.) process integration services. Every layer above can use the functionality provided by the layer below (Figure 3).

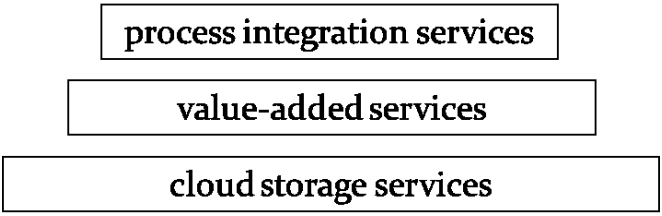

Figure 3: Hierarchical service layers

We assume that services provided by lower layers are reused on higher levels and that the higher layers will not have to re-implement them. If data safe solutions only work within one layer and are not using or providing functionalities to or from other layers, these electronic data safe solutions will face the need for re-adjusting or enlarging their functionalities and services in order to become successful, as explained later. Common to all service layers is their need for a high quality of service: On the one hand, this happens on a technological level (QoS) encompassing security, reliability, availability, etc. (Badger et al. 2012). On the other hand, the entire service quality can be considered like completing an entire transaction on a web portal (Papadomichelaki et al. 2006).

The foundational level is the *(cloud) storage layer* which encapsulates the basic services for storing data and providing data safety and security, e.g. by liberating the end-users to worry about backup procedures to be prepared against data loss. Moreover, access via several devices with possibly automatically transforming the information format of an information item according to the output device, synchronizing and backing up user data in a transparent, OS- and device-agnostic (smartphone, tablet, PC etc.) manner is performed on this service level.

The *value-added services layer* uses functionalities provided by the cloud storage layer. Additional services are offered providing value to the users. These services could be (non-conclusive enumeration): (a) sharing information items, e.g. like picture sharing or sharing thoughts and ideas like in social networks, (b) collaboration components, (c) automated report

generation or data mining services on the information items sent to electronic data safes (for example, Mint, http://www.mint.com) generates statistics on one's expenses), (d) vendor relationship management for exerting informational self-determination by providing mechanisms to manage one's privacy, e.g. like Mydex or Personal, and last but not least (e) data inheritance functionalities, e.g. to ensure that certain information items survive and are transferred or definitively destroyed if a user passes away, for example, as offered by the solution SecureSafe.

The last and topmost level is the *process integration services layer*. Building on the other two layers and their services, an electronic safe can be used to receive and deliver information items to e-government or e-business processes across organizations and is not tied to one (value-added) service provider. For instance, the SecureSafe solution is coupled with a Swiss bank's online banking portal so that the customers receive their electronic statements transmitted directly into the electronic data safe.

Our hierarchical service layer concept goes in line with the notion of vertically and horizontally integrated services with respect to personal information management (Jones 2012) and the more radical suggestions of separating data storage and data use completely (Ates et al. 2011; Mun et al. 2010; Van Kleek et al. 2012): *Vertically integrated services* like Facebook or YouTube are optimized to capture, store and disseminate specific information items under the realm of one single service provider. In contrast, *horizontally integrated services* would decouple the data storage and the value-added services, so that the features could be combined on demand and according to the user's preferences. Using our taxonomy of hierarchical service layers, we are able to group the existing and future electronic data safes solutions.

Nowadays, cloud storage providers like Dropbox or Microsoft's OneDrive are working mostly on layer one which is dealing with storage issues. Few value-added services are offered which prevents these services from being placed into the value-added layer.

On the second layer the *cluster of e-billing consolidators* is working: These services promise to ease the life of customers by fetching electronic bills from various providers (e.g. utility and telecommunication companies with their own portals) and to aggregate them at one place. Additional value is offered either by integrating payment and reminder functionalities or automated data-aggregation into statistics visualizing the personal expenses. In this category, many companies try to compete with each other as well as against many postal companies which are opening up new business opportunities (accenture 2011). Another cluster of applications working on layer two are the *account and inventory management services*: Solutions grouped into this cluster deal prominently with managing personal information items like account data or managing personal inventory, either locally on a single computer like InformationSafe or as a Software-as-a-Service like Reposito (http://www.reposito.com) – which, in the meantime to update this essay, has ceased to exist. The aforementioned service allows using multiple input devices such as PCs, smartphones or tablets to photograph items and to seize and store data – tasks that have to be facilitated by services provided by the (cloud) storage layer. A third cluster working on the level two of our proposed hierarchy of service layers are *personal data stores focusing on VRM*. These solutions adopted the VRM-paradigm that individuals should control their information items consciously and that they can decide and understand why and with whom they share them. Many of these services like Personal or Azigo have been launched in the last year and therefore they still are either in a (closed) beta or "opening soon" phase, like Mydex.

On level three (process integration services) there is one *cluster of solutions which were initially created or are still run by public service organizations and therefore have a deep rooting and inclination towards e-government*. Few of them offer value-added services like, for instance, Mydex that adopted the VRM paradigm and wants to offer integration into e-government processes. Recently, the concept of "Life-Management Platforms" (Kuppinger 2012a) was suggested combining the personal data store/VRM-vision with process integration of electronic data safes (see also chapter 1.6.4).

2.6 Identifying Factors for the Adoption of Electronic Data Safes

This chapter reports on the factors and areas of interest contributing to the adoption of electronic data safes. This is the result of an exploratory research approach whose method is described in chapter 2.3.4. Table 13 and Table 14 summarize our findings by adding the main items of our discussion for each hierarchical service layer with respect to the corresponding dimension.

Cloud storage services: Effects of economy of scale are working on the network effects dimension and people are incentivized to use cloud storage solutions by the possibility of sharing content with others. They expect these cloud storage technologies to be as easily usable as any local storage component (relating to the dimension of effort expectancy). As a facilitating condition, the service provider's reputation and its terms and conditions are identified. E-Boks, although a privately-owned company, is trusted which might be due to the shareholders that are trustworthy organizations per se: Post Danmark and Nets (payment and credit card processing services).

With cloud storage offerings, users expect data to be ubiquitously available, independent of the device used to access the data. Nevertheless, mechanisms to guarantee data security, safety, and privacy are established. As presented in the vision of electronic data safes, only the owner should be able to have access, neither the safe provider nor any other party without the owner's consent. This means, it has to be legally clarified if, at all, or under which circumstances and by which means the government should be granted access to an electronic data safe. This question reflects general security considerations and results in the following design requirements for electronic data safes: The data safe provider will not be able to have access to an individual's data therefore it is impossible to re-issue a "lost" private key which is used to individually encrypt users' data. Or, that every time data is accessed, this is logged for the transparency of the data owner. For example, the data safes of the Service-BW

portal, (formerly) Wuala or (still existing) SecureSafe encrypt each data safe with a unique key managed only by the owner. These security services on the cloud storage layer should be available to the layers above.

Value-added services: Adding additional functionalities to the cloud storage layer generates additional value for the end-users. For example, services offer the collection of documents from different service portals (utility providers, telecommunication companies) and create added-value by automatically generating reports on expenses based on the bills received, as performed by some of the e-billing consolidators like (formerly) Adminium or Doxo.

These functionalities give the users the means, that they can complete a certain task. For instance, managing their passwords and access data, obtaining financial overview or preventing paper clutter by going digital are all tasks touching the dimension of performance expectancy. Moreover, these services might provide ways to structure the information items received, for example, by offering folder structures, tagging mechanisms or full text retrieval – touching the dimension of effort expectancy. E-Boks in Denmark generates added value by helping users to organize their digital mail, for instance, by letting them create folders. Furthermore, information items can be shared with other users.

If the perceived benefits are judged positive, users might also be willing to share anonymously sensitive data. For instance, sharing health information items to allow anonymous data mining with the aim of detecting new insights and advancing science was a scenario an interviewee could imagine and continued: "Data collection and sharing are not bad per se – only what might be done wrong with it." This idea fits the dimension of network effects in relation to the value-added services: User may receive benefits through collaboration and data sharing, for instance using social bookmarking services. Or if they have agreed upon before, their anonymous data is used to collaborate "for them" with the help of data mining.

We also assume that "managing privacy" as proposed by Mydex (2009) will be just one value-added service among others but users are far more

attracted by service offerings helping them to achieve be-goals in respect to the hedonic dimension. Privacy itself will be regarded by the users as a hygiene factor which does not necessarily translate into a competitive advantage for a service provider because it will be expected to exist and work fine. This is also diagnosed in (Ericsson 2012) and the authors of this study conclude that privacy will not "likely be a consumer driven issue, but rather an industry driven one".

Nevertheless, managing one's personal electronic identity (eID) will be certainly a necessity for using some of an electronic data safe's services and this will be judged within the dimension of effort expectancy. Research on eID-security shows (Kubicek and Noack 2010) that the easier and more convenient authentication methods like software certificates or paper based transaction number lists are much more preferred to more complicated and safer authentication mechanisms. If services are created which show clear benefits of taking the pain of doing a more complex authorization, people will accept it. But if benefits are obscure, people will opt for the simpler solution. Existing eID management systems (eIDMS) on a national level should be successfully extended and expanded not only to serve the public sector, but also the private sector (dual use of a single authentication technology).

		Dimensions of observation		
		Effort Expectancy	**Performance Expectancy**	**Facilitating Conditions**
Hierarchical service layers	**Process Integration Services**	---	▪ integration of information items into processes ▪ control an information item's usage ▪ prevent media breaches	▪ legal context (receipt and acceptance of electronic documents) ▪ standardization to provide interoperability
	Value-Added Services	ease of use for: ▪ structuring information items ▪ electronic identity management system (dual use by private and public sector) ▪ granting proper access rights	services must support goal-achievement: ▪ password safes ▪ financial overview by generated reports ▪ inventory management ▪ aggregation of bills and documents to prevent clutter	---
	Cloud Storage Services	▪ as easy as local storage	▪ ubiquitous access (place/device) ▪ data security and safety	▪ reputation of the service provider ▪ terms and conditions

Table 13: Dimensions of observation according to hierarchical service layers (part 1)

		Dimensions of observation	
		Hedonic Aspects	**Network Effects**
Hierarchical service layers	**Process Integration Services**	---	▪ very strong effects if private and public sector are participating
	Value-Added Services	creating positive user experiences ▪ using mobile devices which fit in the users' way of life ▪ support the achievement of "be-goals"	provide collaboration mechanism: ▪ share data voluntarily to collaborate ▪ receive benefits via explicitly granted but anonymous data mining of personal data
	Cloud Storage Services	---	▪ economies of scale ▪ possibility of sharing content

Table 14: Dimensions of observation according to hierarchical service layers (part 2)

For instance, the Austrian citizen card offers an eID-infrastructure based on a smart-card and authentication via mobile phones which potentially every Austrian citizen can use – but only a small number has actually activated this functionality. On the contrary, E-boks in Denmark uses the eID-infrastructure called NemID (easy ID) which has been widely accepted since its introduction in 2010 and which integrates the formerly separated solutions OCES (government-driven) and NetID (banks). This example shows that using convenient mechanisms and creating an infrastructure which can be used by private and public companies leads to a successful adoption. E-Boks acts as an intermediary between customers

and organizations. But there might originate the risk that an intermediary might become obsolete because of the universal authentication infrastructure: Banks running existing e-banking solutions might argue that this easy login is convenient enough for their customers and therefore they want to avoid paying the intermediary for delivering documents the customer could get himself via the existing e-banking channels.

Data transparency is a double-edged sword. If people should be able to exert informational self-determination, controlling the use is one part of the activities. Granting the proper rights, which is assumed to take place more often in the context of electronic data safes, should require as little effort as possible, which touches the dimension of effort expectancy. Some authors argue, that from a cognitive perspective, users have to take an increasing number of decisions with whom they share data which possibly leads to cognitive overload (Narayanan et al. 2012).

Hedonic aspects are dealing with the joy of use. Services provided on the value-added layer therefore should provide a positive user experience. The not anymore existing service Reposito allowed you to create an inventory as easily and joyfully as possible using smartphones. These devices are used as barcode scanners so that a user can forget about typing in product data and the smartphone apps assists in documenting an inventory item and integrating all information in one place. In such a way, hedonic aspects of "be-goals" like documenting one's inventory for the case of accidents overcomes the status of being a cumbersome "do-goal" activity.

Process integration services: On the layer of process integration services, network effects will have strong influences: The more processes are offered, the more users are attracted. E-Boks has 20'000 senders from the private and public sector and it has 5.3 million users (e-Boks 2011).

The vision of electronic data safes (Breitenstrom et al. 2008) suggests that benefits can be achieved if individuals share information items with processes. For example, account or salary statements could be transmitted electronically to the tax office – without having to switch media. This

relates to the dimension performance expectancy. Such integration on the process level stimulates the performance expectation, that users can purposefully use an electronic data safe to achieve goals and keep track where their data is used.

Providing interoperable process chains surmounting organizational boundaries will be a key challenge for the adoption of electronic data safes. People are weary of re-entering the same data on different web sites to accomplish a task (Brustein 2012). If data can be re-used across organizations or across several government agencies, electronic data safe users experience substantial benefits. But as a precondition, technical, semantic, organizational, and legal interoperability (European Commission 2010) must be established. Electronic data safes benefit from standardization initiatives as facilitating conditions.

Storing data online per se has its benefits (as seen in the success of cloud based storage: being able to access or synchronize data from multiple places with multiple devices), but electronic data safes will certainly not be attractive for users when no other benefit is offered. Existing service offerings of electronic data safes with no process integration (for instance, the nowadays out-of-service e-Bürgersafe in Bremen) are actually used far below the expectations of the service providers, as one interviewee stated. Going out of service can be seen as a result of this lack of benefits provided to individuals as customers.

If electronic data safes are able to receive documents or data with legally binding content (e.g. contracts) or documents associated with an objection period, current work practices and processes needs to be supported with electronic data safes in an analogous way – which is a facilitating condition. For instance, if a postal company sends a registered letter in order to document the reception on behalf of the sender, the organizational, legal, and technological tools should be able to offer the same services digitally. From a legal point of view, it should be clear what the consequences of a failed reception are (for example while being on holidays) or if transfer errors occur. In Austria, this has been legally clarified in the Service of Documents Act.

Another factor which will have influence on the facilitating conditions was identified in the legal acceptance of electronic documents. Many laws, e.g. for taxation, require documents to fulfill certain qualities – being original, unaltered and with approved origin. These "paper-world" concepts were transformed into requirements for handling digital documents, adding a lot of complexity like a forced usage of (qualified) digital signatures. Sticking to such rigid mappings of the paper world to the digital world will impose big barriers for the adoption. Rethinking laws and providing "reasonable" and "moderate" ways of handling digital data and documents in a legally conform way will be key facilitators for the adoption of electronic data safes. Using functionalities from lower layers, services can be created or re-designed so that, for example, documents can be "scanned" using a smartphone and delivered to a business process.

2.7 Discussion and Conclusion

With the help of our model of hierarchical service layers that we attributed with dimensions from UTAUT and adding the dimensions of network effects and hedonic aspects, we could gain insights in the current landscape of electronic data safes. This approach allowed us to identify factors and areas of interest which might serve as facilitators or barriers for the adoption of electronic data safes. We assume that the model of hierarchical service layers is so generic that it can be applied in other context where there is a need for decoupling data management and data processing for service provision.

Our sense-making approach was performed in an exploratory stage of research and our findings needs to be validated – ideally by integrating experiences of real users of electronic data safe solutions. So far, only two end-users of electronic data safe solutions have been interviewed. Further research should focus on (potential) end-users and their expectations of electronic data safes. By contrasting their expectations with the current landscape of electronic data safes, design principles could be questioned, refined or newly discovered. The dimensions taken from the UTAUT were considered to be quite helpful during the sense-making

process. Further research is necessary to explain why some constructs on certain hierarchical service levels could not be supported by data and what this implies for the selected dimensions.

With respect to the business models that we have analyzed, no ideal or predominant model emerged that guarantees success. Each solution analyzed has its specific path dependencies based on design choices or business rationales that contribute to a service's widespread usage – or not. Widespread usage could be achieved by mandating EDS usage, as it is the case for E-Boks as a e-government solution in Denmark which also creates problems (cf. Berger 2015). On the contrary, for all other EDS services, the most frequently pursued market penetration strategy is a mixture of increasing the market share of the existing EDS product, and, at the same time, secure dominance in growth markets. The customers voluntarily chose which EDS service they want to use based on the benefits they can realize by using a specific EDS which drives an EDS adoption. This observation can be explained by using our model of hierarchical service layers: All the EDS services need to design their business models by offering (potential) customers value propositions that maximize the customers' benefits and incentivize them to prefer a specific EDS when competing EDS services do also exist. Incentivizing usage is related to crafting a business model that delivers value to the customers, and, at the same time, creates revenues for the EDS provider. This means, that data safe solutions that work exclusively on one hierarchical service layer and do not integrate the previous ones, they will become vertically integrated solutions or islands where potential benefits for customers might be hard to achieve: For example, this happens if an electronic data safe does not have any data sharing capabilities or data cannot be transferred to processes (which needs to be addressed in an adequate partner/relationship management from a business model perspective). Therefore, it is necessary that successful services will use functionalities provided from lower levels of our model of hierarchical service layers. For instance, services can be created or re-designed so that documents can be "scanned" using a smartphone and later on delivered to a business process, which is provided as functionality on a higher level. Such additional functionalities

serve as value propositions helping to discern the different EDS service providers to achieve a sound business model.

To synthesize our findings, we conclude that clearly perceivable benefits are the key facilitators for the adoption of electronic data safes arising from the UTAUT dimensions of performance and effort expectancy. As implications for practice, we suggest that electronic data safe solutions should put emphasis on their ease of use. Furthermore, value-added services should be developed that appeal to hedonic aspects but at the same time contribute to users' demands originating from the dimension of performance and effort expectancy. All these value-added services should be able, if necessary, to be integrated into business processes in order that users can achieve "be-goals" and not only "do-goals".

2.8 Appendix: Service Business Model Canvases

This chapter serves as an appendix to the first essay providing detailed information about the EDS services' business models using the Service Business Model Canvas (SBMC) as described in chapter 2.4. In the following tables, the business model is analyzed from the perspective of the customer (CST), the focal company (FC), and the platform partners (PP).

SecureSafe						
Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST		FC			PP	
* freemium model with different tiers based upon storage volume * private individuals: yearly usage fee depending upon the amount of storage needed * business customers: per individual and base fee	* compatible devices * conviction/need to store personal data in the cloud * trust in storage provider	* registration * payment for service * configuration/setup * authentication * storing information items * accessing information items * sharing information items	* mobile access to inform. items * encrypted storage * non-US service * password safe & file safe * choice of security level for authentication (2-factor or not) * automatic synchronization * cloud storage as backup * controlled hand-over of information items after one's death (digital inheritance) * secure file sharing with individuals or teams & document reception	* self-service for registration and use	* website * smartphone apps * syncing client	* time savings by automatic synchronization or backup ?
* marketing / business development * operations * SW development * staff	* staff * servers located in CH * software infrastructure Swiss made * 2-factor authentification * automated billing (credit cards, online banking) * trust inference by working with highly trusted organizations (banks) * API for document delivery	* registration * providing secure storage (infrastructure, apps) * operations * product/service development * billing * support * partner management (acquisition, legal, technological, financial)	* safe storage solution * encrypted storage * server location: CH = non-US * easy access of information items over devices for individuals or teams * data inheritance * secured electronic document delivery * Swiss made	* automated for majority of private individuals * support for private individuals * taylored solutions for business customers * taylored solutions for document providers* safe storage solution * encrypted storage * server location: CH = non-US * easy access of information items * indirect relation with individuals as the recipients of documents (GUI is SecureSafe branded) * give away interface for document delivery/access to SecureSafe	* website * smartphone apps * syncing client	* freemium model * usage fees (yearly, per user) * per delivered document * custom developments priced seperately
* service fee for document delivery * setup costs and maintenance costs for connecting back-end systems for document delivery into SecureSafe	(partners: document providers) * backend systems connected to SecureSafe for document delivery * staff * benefits due to electronic document delivery	(document providers) * document delivery to SecureSafe using its API	* deliver documents securely * no need to develop and run an own document delivery infrastructure * provide a modern service to customers (unified data storage) * secured transfer of documents to a customer's inbox		* backend systems for document delivery into SecureSafe	* fees from customers

Table 15: Service Business Model Canvas for SecureSafe

DocSafe							
	Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST	* private individuals: free (fair use policy)	* compatible devices * conviction/need to store personal data in the cloud * Swisscom Login * accounts with vendors participating in doxo	* registration * configuration/setup * authentication (Swisscom Login) * storing information items * accessing information items * sharing information items * transfer DocsafeID to potential partnerns/document senders for delivery	* mobile access to inform. items * encrypted storage * user-managed access * non-US service * password safe & file safe * electronic version of the previously paper-based archive * bundled with possibility to receive documents electronically * upload assistant * cloud storage as backup * controlled hand-over of information items after one's death (digital inheritance) * secure file sharing	* self-service for registration and use	* website * smartphone apps * upload client	* time savings by having everything at one place?
FC	* marketing / business development * operations * SW development * staff * outsourced activities	* staff * servers located in CH * software infrastructure * Swisscom Login * API for document delivery	* registration * providing secure storage (infrastructure, apps) * operations * product/service development * support * management of outsourced activites / partners (e.g. data center, external developers) * partner management (acquisition, legal, technological,	* positioning Swisscom as a modern service provider * aiming at becomung the hub for personal information management for individuals * positive image of Docsafe transmits itself to the Swisscom brand and its products * replacing paper-based communication via secure electronic communication * providing a unified online channel for document reception (and transaction) * advocate for the privacy of users (user-managed access)	* automated for majority of private individuals * exploiting existing customer relationship and Swisscom brand power * support for private individuals * taylored solutions for business customers * taylored solutions for document providers*	* website * smartphone apps * upload client	* cross financing with other Swisscom services * per document delivery fee based upon different tiers per month
PP	* per document delivery fee based upon different tiers per month * setup costs and maintenance costs for connecting back-end systems for document delivery into DocSafe	(partners: document providers) * backend systems connected to Docsafe for document delivery * staff * legal expertise * benefits due to electronic document delivery	(document providers) * document delivery to Docsafe customers using its API for invoices etc. * provide support for output management systems	* cheaper document delivery than standard conventional, paper-based mail * speed of delivery * no need to develop and run an own document delivery infrastructure * authenticated customers * secured transfer of documents to a customer's inbox	* have partner's processes or interfaces integrated within Docsafe * determine the level of visibility in the Docsafe portal of the partner's portal	* backend systems for document delivery into Docsafe * partner GUI elements	* fees from customers

Table 16: Service Business Model Canvas for DocSafe

e-Tresor							
	Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST	* usage fee (monthly 12 EUR) for the e-Tresor (5 GB) * free (2 GB) for the Handy-Signaturkonto	* compatible devices * conviction/need to store personal data in the cloud * Handy-Signatur Konto * trust in storage provider	* registration * configuration/setup * authentication (Handy-Signaturkonto) * storing information items * signing documents (and invoices) * accessing information items * sharing information items	* mobile access to information items * encrypted storage * user-managed access * non-US service * password safe & file safe * sign documents electronically * secure file sharing with individuals or teams	* self-service for registration and use	* website	* time savings?
FC	* marketing / business development * operations * SW development * staff	* staff * servers located in AT * software infrastructure * Handy-Signatur Konto (eID solution) * automated billing * maintain funding	* registration * providing secure storage (infrastructure, apps) * operations * product/service development * support * management of outsourced activites / partners (e.g. data center, external developers) * partner management (acquisition, legal, technological, financial)	* provide secure storage for documents * signing documents to contribute to going digital in the private and the public sector (electronic document delivery)	* automated service delivery * support for users* provide secure storage for documents * signing documents to contribute to going digital in the private and the public sector (electronic document delivery)	* website	* usage fees (12 EUR/month)
PP	* no data found if document delivery for partners is associated with fees or if they use the email alias for free	* benefits due to electronic document delivery	* backend systems need to adapted to deliver documents/output into the e-Tresor	* infrastructure component for the Handy-Signatur for heavy users	* not applicable	* offline * backend systems for document delivery?	* taxes

Table 17: Service Business Model Canvas for e-Tresor

Service-BW							
Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST						
* free	* compatible devices * conviction/need to store personal data in the cloud * trust in storage provider	* registration * configuration/setup * authentication (account/eID passport) * storing information items * accessing information items * sharing information items	* mobile access to information items * encrypted storage * user-managed access * non-US service * store documents electronically * reuse electronic documents in e-government processes (future) * e-government portal *secure file sharing	* self-service for registration and use * mostly with governmental organizations on a municipal level; tendency to have more centralized e-government activities on an state level	* website	* time savings?
FC						
* staff * funding to pay for outsourced activities (SW development, operations)	* staff * officially mandate by the federal state's government (entails funding) * servers located in Germany * quasi monopoly on e-government in Baden-Württemberg on a state level * combination with the electronic ID function of the German passport	* product/service development * management of outsourced activites / partners (e.g. data center, external developers) * promoting e-government in the state of Baden-Württemberg on a state and municipal/county level	* single portal for e-government transactions * (single) electronic identity throughout all e-government services * electronic document delivery * electronic forms * e-payment * process management	* automated service delivery (document safe)* single portal for e-government transactions * (single) electronic identity throughout all e-government services * electronic document delivery * electronic forms * e-payment * process management	*website	* taxes
PP						
* operations * SW development	(partners: SW development and operations) * staff * servers * software infrastructure * infrastructure provided by the state of Baden-Württemberg provided to subsequent organizational units	(contractors - external) * product/service development * providing secure storage (infrastructure) and an e-government portal * operations * reuse of identity or process data initiated through the Service-BW portal	* cost reduction due to centralized service provision by the state (no need to duplicate services on a municipal level)	* future: direct citizens more to self-services on the Internet	* backend systems coupled with the Service-BW portal?	* taxes

Table 18: Service Business Model Canvas for Service-BW

doMap

Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST						
* free * fees for services might apply	* compatible devices * conviction/need to store personal data in the cloud * trust in storage provider	* registration * configuration/setup * authentication (account/eID passport) * contributing information items for certain e-government processes * access results /documents electronically * e-payment	* start e-government transactions from anywhere * get results of e-government transactions transmitted in an inbox * single point of contact for e-government in the city of Dortmund	* self-service for registration and use	* website	* time savings?
FC						
* staff * outsourced activites (SW development, operations)	* staff * officially mandate by the municipal government (entails funding) * quasi monopoly on e-government services in the city of Dortmund	* product/service development * management of outsourced activites / partners (e.g. data center, external developers) * billing with electronic Lastschrift	* single portal for e-government transactions * (single) electronic identity throughout all e-government services * electronic document delivery * electronic forms * e-payment * process management	* automated service delivery * support (service hotline)* single portal for e-government transactions * (single) electronic identity throughout all e-government services * electronic document delivery * electronic forms * e-payment * process management	*website	* taxes * service fees
PP						
* operations * SW development	(partners: SW development and operations) * staff * servers * software infrastructure	(contractors - inhouse) * product/service development * providing e-government portal functionality (infrastructure) * operations	* not applicable	* not applicable	*not applicable	* not applicable

Table 19: Service Business Model Canvas for doMap

e-Boks							
Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST			FC			PP	
* free	* compatible devices * NemID	* registration * configuration/setup (select senders) * authentication * checking the centralized, digital post box (finance, government) mandated by the Danish Government * accessing information items * seldomly sharing information items	* having all important documents at one location * reduce clutter at home * save time * non-US service * b/g2c communication * b/g2b communication	* self-service for registration and use	* website * mobile apps	* time savings?
* marketing / business development * operations if not outsourced * SW development if inhouse * outsourced activities (operations?, SW development?) * API for document delivery	* staff * NemID * servers * software * connections to document providers * governmental approval for running the infrastructure	* product/service development * management of outsourced activites / partners (e.g. data center, external developers) * support	* provide a single point for receiving electronic documents sent by private and public sector companies for Danish citizens and legal entities (mandated e-government) * cheaper document delivery * faster document delivery * certified mail system	* automated service delivery for citizens and legal entities * support * relationship with document providers* provide a single point for receiving electronic documents sent by private and public sector companies for Danish citizens and legal entities (mandated e-government) * cheap doc. delivery	* website * mobile apps	* service fees from document senders
* per document delivery fee	* central business register (unique ID for businesses) * central person register (unique ID for individuals) * NemID (software-based certificate used in the private and public sector, as well)	(contractors - external) * operations (document providers) * document delivery	* reduction in postage fees	* defined processes upon development and operations of the e-Boks service with 3rd party providers * close relations with Danish e-government to maintain its status as the single e-Boks provider	* backend systems for document delivery	* project funding for development * service fees for operations

Table 20: Service Business Model Canvas for e-Boks

Doxo							
	Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST	* free	* compatible devices * accounts with vendors participating in doxo	* registration * configuration/setup (select bill providers) * authentication * storing information items * accessing information items	* all your accounts in one place * all bills in one place * all payments in one place * digital filing cabinet service	* self-service for registration and use	* website	* time savings?
FC	* marketing / business development * infrastructure (servers, licences) * operations * SW development	* staff * software * servers * connections to document providers	* product/service development * management of outsourced activites / partners (external developers, service providers) * acquisition of new bill providers	* paperless billing and bill pay service * access all accounts under one login (doxo) * store important files from providers at one place	* automated service delivery * relationship with bill providers* paperless billing and bill pay service * access all accounts under one login (doxo) * store important files from providers at one place	* website	* service fees from payment recipents?
PP	* not applicable	(partners: document providers) * bills processable via doxo * legal expertise * benefits due to electronic document delivery	(document providers) * provice access to doxo via API		* accepting payments made via doxo	* website? * API	* indirectly from customers * discourage customers to use doxo due to necessitated fee payment by the bill providers (otherwise

Table 21: Service Business Model Canvas for Doxo

Volly							
	Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST	* free	* compatible devices * accounts with document senders using inlet	* registration with inlet either directly with intlet or with the service provider white labelling inlet * authentication * accessing information items * make payments	* all important documents at one place * coupled with e-payment functionality * information items are accessible from everywhere	* self-service for use * (registration: indirectly)	* website * app	* time savings * less efort
FC	* marketing / business development * operations * SW development * staff * API for document delivery	* staff * software * servers * connections to document providers	* product/service development * management of outsourced activites / partners (external developers, service providers) * acquisition of new document providers	* provide a platform for paperless document delivery and billing * permission-based and interest-based marketing * assisting companies and individuals to go paperless	* automated servie delivery * relationship with bill providers* provide a platform for paperless document delivery and billing * permission-based and interest-based marketing * assisting companies and individuals to go paperless	* website * API	* per document delivery fee? * service fees to establish initial connect? ==> Not made public yet.
PP	* per document delivery fee	(partners: document providers) * provide documents to inlet * staff * legal expertise * benefits due to electronic document delivery	(document providers) * deliver documents to inlet via its API	* reach customers where they are * no need for setting up an own infrastructure for document delivery, storage and e-payment * reduction in customer support costs * branded landing page and pages with dedicated marketing and customer support space	* accepting payments made via inlet	* API	* indirectly from customers

Table 22: Service Business Model Canvas for Volly

Mydex

Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST						
* free	* compatible devices * accounts with companies participating in Mydex	* registration * configuration/setup * authentication * storing information items * accessing information items	* sharing of information items according to the user-managed access paradigm * all information items in one place (snippets) * all bills in one place * all payments in one place * could involve a digital filing cabinet service * keep private data safe	* self-service for registration and use	* website	* time savings?
FC						
* marketing / business development * operations * SW development * staff * API for document delivery	* staff * software * servers * connections to document providers * licensed as a Community Interest Company (signal trust/endurance/	* product/service development * management of outsourced activites / partners (external developers, service providers) * acquisition of new connecting organizations	* provide a platform (personal data store) for carrying out transactions with personal data under the user-managed access paradigm * working with the British Government to become an e-Identity provider (sharing with trusted status) * Community Interest Company acts in the interest of individuals = neutral * being a fair data handler (awarded by a marketing association)	* automated service delivery * relationship with connecting companies to use Mydex® provide a platform (personal data store) for carrying out transactions with personal data under the user-managed access paradigm * working with the British Government to become an e-Identity provider	* website	* one time connection fee * connection fees in tiers according to connected customers * yearly service fee * per document fee
PP						
* one time connection fee * connection fees in tiers according to connected customers * yearly service fee * per document fee	(partners: document providers) * provide documents to Mydex * staff * legal expertise * benefits due to electronic document delivery	(document providers) * use Mydex API to interact with customers	* reuse "trusted" personal data/information items	* exchange personal data / information items via the Mydex API	* API * connecting partner's backend systems to Mydex platform	* indirectly from customers

Table 23: Service Business Model Canvas for Mydex

Personal / teamdata							
Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
* fees per team size	* compatible devices	* registration * configuration/setup * authentication * adding information items * accessing information items	* reuse existing information in a team * time savings	* selv-service for registration and use * support depending upon pricing scheme	* website	* time savings?
* marketing / business development * operations * SW development * staff	* staff * software * servers	* product/service development * operations * management of outsourced activites (external developers)	* provide a platform to store information items for team use with granular access rights on a user-managed access paradigm	* automated service delivery * support when requested and according to bought product* provide a platform to store information items for team use with granular access rights on a user-managed access paradigm	* website	* service fees based on team size
	* not applicable anymore after strategy shift away from PDS					
CST	FC	PP				

Table 24: Service Business Model Canvas for Personal / teamdata

Azigo							
Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST						
* free	* compatible devices * accepted methods of payment	* registration * configuration/setup * authentication * initiating purchases via Azigo instead of going to the merchant directly	* receiving marketing-related offers in one place * enjoy benefits from loyalty or reward programs * selectively subscribe to companies which are really interesting to a customer's profile/needs --> targeted marketing	* self-service for registration and use	* website	* rewards / benefits from loyalty programs
FC						
* marketing / business development * operations * SW development * staff	* staff * software * servers * connections to financial institutions and member based groups = partners	* product/service development * management of outsourced activites / partners (external developers, service providers) * acquisition of new partners	* provide a platform to distribute rewards and benefits from loyalty programs to the customers automatically * provide the individuals as users with the power to select the marketing information they want * provide the partners with the ability to send targeted ads to registered users	*automated service delivery * relationship with partners in rewards and loyalty programs* provide a platform to distribute rewards and benefits from loyalty programs to the customers automatically * provide the individuals as users with the power to select the marketing information they	* website	* average 7.5% commission for user's purchases initated through AZIGO
PP						
* average: 7.5% commission for user's purchases initiated on the Azigo platform	* offering a rewards or loyalty programm to tie customers to their services * use API to deliver documents to customers * benefits due to electronic document delivery	(document providers) * use AZIGO API to deliver documents and offers to customers	* more targeted offers for customers * stop annoying customers by interacting / sending them marketing offers directly (pull instead of push) --> image of being more consumer-oriented // following the VRM paradigm	* exchange personal data / information items via Azigo * leads generated by Azigo will be transferred to the partners to carry out the transaction	* API * connecting partner's backend systems to AZIGO	* indirectly from customers

Table 25: Service Business Model Canvas for Azigo

Qiy							
	Cost Structure	Key Resources	Key Activities	Value Proposition	Relationship	Channels	Revenue Streams
CST	* membership fees * license fees to QIY foundation to use its scheme	* compatible backend systems to use the QIY scheme	* registering * using QIY API in backend	* obtaining verified data * proposing VRM as an assett to customers (data scarcity) * benefit from centralized data access	* close contractual relationships (becoming a member of QIY foundation) * self-service by employing QIY api	* API	* indirectly paid by individuals as customers
FC	* marketing / business development * operations * SW development * staff	* intellectual property: QIY scheme (QIY Trust Framework) licensed to use (= platform?) * staff * software * server * connections to service providers / trust partners	* product/service development * management of outsourced activites / partners (external developers, service providers) * acquisition of new partners	* provide a platform (scheme) for centralized data storage and management under the user-managed access paradigm for individuals * provide verified data to service providers	* automated service delivery * relationship with partners to use QIY scheme* provide a platform (scheme) for centralized data storage and management under the user-managed access paradigm for individuals * provide verified data to service providers	* website * mobile apps * API	* service fees * membership fees
PP	* indirectly charged by the service provider	(partners: document/data providers) * compatible devices * staff * provide documents/data to Qiy * use Qiy-API * benefits due to electronic document /data delivery or usage	(document providers) * authenticate via the QIY infrastructure for services * trust service providers that QIY works in the background	* benefit from user-managed access and controlling one's data again	* using QIY scheme elements to interact with service providers over the QIY platform	* website	* not applicable

Table 26: Service Business Model Canvas for Qiy

3 Current Usage of an EDS (Essay 2)

This essay is based on the following peer-reviewed conference paper:

Pfister, Joachim; Schwabe, Gerhard (2016): „Going Paperless with Electronic Data Safes: Information Ecology Fit and Challenges". In: Proceedings of the Thirty Seventh International Conference on Information Systems. December 11 – December 14 2016. Dublin, Ireland.

Abstract

In private households, once received paper-based documents are increasingly substituted by electronic documents. In order to "get organized", an individual nowadays needs to oversee a plethora of digital and physical information items stored at various locations. As a technological solution, cloud-based storage services such as an Electronic Data Safe (EDS) emerge as a home for all digital valuables. In this paper, we analyze how such an EDS fits into an individual's information ecology by drawing upon the results of a qualitative interview study with 39 users of three different EDS services. We develop a typology of the content that is kept safe in an EDS, reflect upon the motivations and upon an EDS's role with respect to other cloud-based storage services individuals are using. The challenges of maintaining a digital, personal archive are depicted and "data value zones" are introduced as a sensitizing concept to reflect upon problematic areas.

3.1 Motivation and Research Goal

Information fragmentation (Karger 2007) is an ongoing challenge in Personal Information Management (PIM) (Jones and Teevan 2007b): The personal space of information (PSI), that spans various collections of information items, is nowadays distributed over devices, as well as physical and virtual storage locations, such as cloud storage or software-as-a-service offerings (Jones 2015). Besides, information items in their physical form are still an important part of an individual's PSI. It is up to each of us to "get organized" and develop strategies for keeping, finding, maintaining, and organizing information items in the digital and the physical world (Jones and Teevan 2007b). New services are offered to help safeguard important electronic (or physically born but now digitized) information items, such as multi-purpose, cloud-based file storage services or "Electronic Data Safes" (EDS) (Pfister and Schwabe 2013). These EDS are promoted as the quasi-natural habitat for all "information item valuables" serving as the digital equivalent of a secure filing and organization system for formerly paper-based documents. Moreover, an EDS offers functionalities to receive electronic documents from authorized senders thus serving as another mailbox. An EDS offers features adding supplementary levels of security compared to "ordinary" cloud storage offerings: For example, two-factor authentication and a server-side encryption with a user-specific key are implemented, so that the provider cannot access the data in his data centers (cf. Borgmann et al. 2012).

Electronic document delivery is continually substituting physical letters and there is an obvious trend for going paperless in B2B, G2B and also in the B2C or G2C context: In the postal sector, e-substitution leads to a falling volume of letter mail by almost a quarter since 2004; in 2014 the total mail volume declined by 3.9% on average (International Post Corporation 2015). Therefore, postal service providers as intermediaries are facing tremendous challenges by the ongoing digitization. Besides a reduction in transaction costs for the senders, the recipients of electronic communications (may) benefit from lowered costs for services, a more-

timely information provisioning or realizing the dream of a paperless (home) office – something which has been described as a myth in the professional office (Sellen and Harper 2002). Nowadays, information items are directed towards individuals via several different channels which, in turn, contribute to a further fragmentation of an individual's PSI. It is still unclear and has been a blind spot in research so far what PIM strategies are developed by individuals as recipients of such digital documents to cope with this externally enforced trend towards digitization – and how compatible this trend is with already existing personal practices and motivations to curate information items digitally in one's PSI. We want to understand how an EDS is currently used in the field by end users and how it fits in their existing PSI leading to our research question: *Which role does an EDS have in an individual's information ecology?*

In order to answer our research question, we follow an interpretive approach by first trying to understand which content and why users selected this content to be stored in a "safe place". Then, we ask how the EDS fits into the bigger picture of an individual's information ecology. Therefore, we interviewed 39 users of EDS services using a semi-structured interview guide. This resulted in 53 hours of audio data that was transcribed and analyzed using a thematic analysis approach. We invited the participants to give a guided tour in their otherwise inaccessible EDS by letting them voluntarily describe the information items stored therein when they had their EDS opened in front of them during the interviews. Moreover, the participants provided rich descriptions of their information ecology, for instance, which devices and services they use to keep their information items flowing and safe.

Our research is related to "practice theory". Originating in sociology, the turn towards analyzing "practices" (Schatzki et al. 2001) was continuously embraced in other disciplines, such as IS (Cecez-Kecmanovic et al. 2014; Kuutti 2013; Tavakoli and Schlagwein 2016). There is no single "practice theory" but they are considered as a family of approaches sharing historical and conceptual elements (Kuutti 2013; Tavakoli and

Schlagwein 2016). Instead of separating the object and subject, practice theory focusses on the entangled relationship between these two entities that are performed in practices which are "[...] routines consisting of a number of interconnected and inseparable elements: physical and mental activities of human bodies, material environment, artifacts and their use, context that contain understanding, human capabilities, affinities and motivation. Practices are wholes whose existence is dependent of the temporal interconnection of all these, and that cannot be reduced to or explained with any one single element." (Kuutti 2013) Following this school of thought, current PIM activities are then practices that are performed by agents using the human body's or the artifact's materiality. In order understand these practices, it is insufficient to focus on micro-interactions, for example, only related to one specific service; the context in which these practices are performed needs also to be taken into account. To achieve this, we based our research on the widely used concept of an *information ecology* (Davenport and Prusak 1997; Fidel 2012; Nardi and O'Day 2000) to analyze and describe human practices (but without relating it to practice theory). In Human-Computer Interaction (HCI), the perspective of an ecology was used to inform the analysis and design of interactive artifacts that transcend individual use by taking into account the complex digital and non-digital context made up by other users and various technological resources (Blevis et al. 2015; Bødker and Klokmose 2012; Jung et al. 2008). As information technology permeates in the private domain and each individual forms part of various socio-technical entanglements, an information ecology perspective allows us to research the relationships between the people who are using technology, the technology itself and how practices are shaped.

An information ecology is conceptualized as "a system of people, practices, values and technologies in a particular environment" (Nardi and O'Day 2000, p. 50). Within such an information ecology, continuous evolution takes place by the multiple levels of influence, for example, if one aspect of the system changes, its effects can be experienced throughout the whole system (Yvette Blount 2011). Such an ecology perspective has not yet been applied to an individual's PIM activities as the "particular

domain" which is characterized by information fragmentation. We argue that it is necessary to understand the whole ecosystem of an individual, not only the interaction with single artifacts or services, to identify future design possibilities for PIM activities and services. In doing so, we will gain an understanding of how EDS services fit into the existing landscape of human practices and tools for managing one's PSI. These insights will help designers to develop solutions that reduce frictions in an individual's information ecology, especially when both, the service providers and the individuals, are aiming for going paperless.

The intended audience of this paper are, besides researchers in the domain of PIM, service providers of cloud storage solutions in general, EDS service providers, and organizations in the B2C or G2C context that send information items directly via their portals or services to individuals. Generally speaking, our research addresses every contributor of information items who cares about delivering its services in a user-centered way to alleviate the problem of information fragmentation.

The research contributions of this paper are twofold: First, our findings describe PIM practices with respect to "practice theory". Thereby, we expand the body of literature in PIM on digital possessions through a deeper understanding of users' notions what valuable digital possession are, why they were created or saved from other sources and where they are stored. Second, we introduce the concept of "data value zones". We suggest this as a sensitizing concept for future research involving cloud storage services that provide individualized storage and the ability to share information items. This concept helped us to reflect productively upon challenges we observed empirically in our data.

The remainder of the paper is structured as follows: After presenting related work from the PIM domain and expanding on the concept of an EDS, we present our research context and the approach for data collection and data analysis. Then, findings are described: We start with an insider's view on the types of content before reporting on the user's motivations and portraying their information ecology. Then, the challenges of individuals aiming for a paperless personal archive are presented. In the

discussion chapter, we reflect upon an EDS place in the information ecology. Thereby, we introduce our concept of "data value zones" and discuss some challenges in the field to illustrate its practical relevance as a sensitizing concept.

3.2 Related Work

Related work on personal information management has been introduced in the synopsis chapter (see chapter 1.6.2) as well as for electronic data safes (see chapter 1.6.4).

Personal cloud storage services such as Dropbox or GoogleDrive enjoy widespread usage whereas services putting a higher emphasis on security with server-side or client-side encryption, such as Wuala (stopped its operation in November 2015), SpiderOak, or TresorIt (all using the concept of zero-knowledge) seem to be more known and used by security risk-averse users. We posit that an electronic data safe (see chapter 1.6.4) is also a personal cloud storage service because of its ability to upload diverse file formats and being accessible through many devices. It has the potential of being used for sharing documents and files stored therein, but sharing is not mandated. It is offered as one functionality of a cloud-based storage amongst other functionalities such as ubiquitous access, synchronization over devices, and collaboration (Marshall and Tang 2012; Voida et al. 2013). We are not aware of prior research investigating the content of an EDS or a trustworthy cloud storage provider.

The mailbox and transactional aspects of an EDS can be related to the domain of electronic bill presentment and payment (EBPP) and electronic document delivery by postal services. As noted by Hildebrand (2015), a possible transition path is evident: from (1) manual invoices sent by postal letters, (2) to semi-automated processes using PDF documents as invoices sent by e-mail or through provider specific portals, and (3) to, finally, a fully, end-to-end integrated order-to-payment process. For the senders, electronic documents have huge advantages by reducing transaction costs. However, on the recipient's side, it has not yet been

investigated whether "going digital" reduces transaction costs in form of a less burdensome PIM. Our study helps to understand what role does an EDS play when end-users have to organize electronic documents – and still are bound to manage existing or still newly arriving physical documents at the same time.

3.3 Research Method and Empirical Context

3.3.1 Empirical Context

Semi-structured interviews were used to collect data from 39 users of three EDS services. These three EDS service providers were contacted by the authors of this paper and asked if they supported this interview study by helping to recruit participants. Two of these service providers are Swiss based and are run by private companies (service A and B). The third EDS provider (service C) is part of the Austrian E-Government infrastructure and is run by a private sector company. The authors of this paper worked independently from the participating EDS service providers; no conflict of interest or financial dependencies existed.

EDS service A is marketed as a safe location for storing documents and passwords to access them everywhere. The service is offered for free and native apps for iOS and Android are provided but no client for automatically synchronizing documents. *EDS service B* presents itself as a general purpose, secure online storage provider following a freemium pricing model. A password safe is offered and, as well as for the files, it is accessible via native iOS and Android apps. This service offers a client for synchronizing files automatically over various platforms. *EDS service C* is provided as a data safe within the context of the Austrian e-government infrastructure. It is bundled with an e-identity component of a digital signature and has got a freemium pricing model offering a safe space for storing and digitally signing documents.

The participants were recruited by self-selection and answering open calls for participation in an interview study advertised for about ten days

either on the EDS's login page (service B) or announced in the news section after logging in (service A). The participants were offered a small gift. This resulted in the recruitment of 20 (EDS service A) and 16 (EDS service B) participants. For EDS service C, recruitment took place using an open call for participation on Facebook offering a small gift which three participants welcomed. The interviews were carried out via Skype, Google Hangout or telephone except for two interviews that took place in the participants' homes due to geographical proximity where the researchers were located.

3.3.2 Data Collection

The interview guide for performing the semi-structured interviews has been pre-tested to optimize the wording and flow of the questions and to ensure a reasonable length-depth ratio of the interviews. The interviews were audio-recorded. After asking some demographic data, the participants were invited to *draw their information ecology*, an approach that was inspired by Kaye et al. (2014). By asking "Where do you store digital information in the cloud?" and letting the participants draw their information ecology, they were better able to reflect upon the services they used. Then, the participants were asked to *give a guided tour* of their electronic data safe and its content, an established and widely used method of inquiry in the domain of PIM (Jones 2015). Therefore, the interviewees had opened their data safe during the interview. They were given full control over their privacy and confidentiality by only telling the interviewer about the content elements that they felt safe of. The interviews continued by asking about practices surrounding the reception and the processing of electronic documents, and how paper is handled.

In total, 39 interviews have been conducted (31 in German, 8 in English) resulting in 53 hours and 02 minutes of audio data. One of the authors transcribed all the interviews. On average, an interview's duration is 1 hour 19 minutes and it contains a net number of 4079 words without the questions asked.

ID	age	gender	profession
A01	59	w	pharmaceutic administrator
A02	51	m	project lead public transport
A03	51	m	coaching/consulting in IT
A04	48	m	trainer for Asian sports
A05	29	m	supporter IT
A06	47	m	policeman
A07	30	m	software developer
A08	54	m	team lead in a telco
A09	46	m	study manager nutrition com
A10	64	m	teacher
A11	57	m	ERP consultant
A12	42	m	consultant banking
A13	27	m	electrical engineer
A14	34	w	office employee
A15	63	m	professor IT, pensioned
A16	37	m	advocate
A17	43	m	sales representative
A18	28	m	informatics employee
A19	39	m	software developer
A20	54	m	toxicologist
B01	44	m	financial clerk
B02	44	m	fire inspector
B03	34	m	technician heating
B04	48	m	consultant IT security
B05	42	m	IT manager
B06	63	m	camera operator, pensioned
B07	56	m	director of an IT company
B08	53	m	program lead in a bank
B09	47	m	educator
B10	32	m	event manager, IT consultant
B11	46	m	IT consultant, freelancer
B12	33	m	IT consultant
B13	39	m	IT security engineer
B14	52	m	electrical engineer
B15	49	m	consultant for banks
B16	44	m	IT director
C01	33	w	public relations representative
C02	25	w	public relations representative
C03	41	w	consultant e-government

Table 27: Detailed description of the participants

The participants came, due to their self-selection, from various backgrounds and had in common that they actually used a specific EDS. 34 males and five females took part and the average age is 41 years (25-29: 4; 30-34: 6; 35-39: 3; 40-44: 7; 45-49: 7; 50-54: 6; 55-59: 3; 60-64: 3). Everyone used at least one smartphone. For a more detailed description of the participants, please see Table 27.

3.3.3 Data Analysis and Interpretation

After the transcription of the interviews, thematic analysis (Braun and Clarke 2006) as a method for analyzing the interview data was used to answer our research question: *Which role does an EDS have in an individual's information ecology?* This method has been successfully employed as an interpretive research paradigm in HCI (Vincent et al. 2014) to uncover themes systematically. The method is closely related to grounded theory (Glaser and Strauss 2009; A. Strauss and Corbin 1998) and it can be used in a realist (essentialist) or interpretive (constructionist) way. Its principles are equivalent to a hermeneutic approach. The research in this study is conducted within a constructionist framework. We proceeded inductively in a data-driven fashion without an apriori attempt to fit the data into theory. Thus, observations are interpreted to uncover latent themes – to use the terminology of Braun and Clarke (2006). They represent hypotheses about underlying motives why certain information items are stored in an EDS. Furthermore, they indicate how an EDS fits into an individual's information ecology. We conceive that the positioning of services in an information ecology is related to existing and newly developed or adapted practices.

To maintain rigor, we followed the six phases as described by Braun and Clarke (2006): The interviews, as well as the transcription, were conducted by the first author of this paper which allowed him to immerse deeply in the data by performing these steps himself and re-reading the data several times (phase 1: familiarize with the data). The analysis was assisted by using the software MAXQDA. Initial codes were assigned using open coding (phase 2). Axial coding was used to identify themes by collecting codes into potential themes (phase 3). Internal validity was

assured by iterating between identified concepts, the assigned codes, and themes several times, paying attention to reflect upon the researchers own perceptions and preconditions that might influence the research process (phase 4: reviewing themes). We did not opt for coding the data set independently by another researcher based on the understanding of coding as an active and reflexive process and that no exclusive reality in the data can be captured by assigning codes which would be more a realist assumption. An internal research report was written by the first author which served as a means to define and name themes (phase 5 and phase 6). Then, discussion with research peers and the other author proceeded to validate and refine the discovered themes before this essay was compiled.

The aforementioned six phases do also cover the criteria for qualitative research conducted in information systems research developed by Klein and Myers (1999): (1.) "The fundamental principle of the hermeneutic circle" is achieved by iterating between data, composing intermediate reports and discussing the results with peers. This is covered by phases 4, 5, 6 of Braun and Clarke. (2.) "The principle of contextualization": By relating our findings to prior research in the domain of PIM and asking our participants questions about other services besides going in-depth into their EDS usage, we were able to contextualize our findings. This is covered by phase 5 and 6 of Braun and Clarke. (3.) "The principle of interaction between the researchers and the subjects": In preparing the interview guide and pre-testing it, we gained initial experience in how the interview study participants would react. During the interviews and the analysis, we paid attention that the observations guided the sense-making process and not own assumptions. This is related to Braun and Clarke's phases 1, 2, 3, and 4. (4.) "The principle of abstraction and generalization": During the analysis, we related our findings to existing theories of PIM and discussed them in the light of an "information ecology". This refers to refining the findings in phase 6 referenced by Braun and Clarke. (5.) "The principle of dialogical reasoning": Our analysis was not guided by preconceptions. We paid attention to let the themes develop from the data and anchor them therein. This took place by discussing

emerging themes with peers and compiling intermediate reports. This is related to phases 4, 5 and 6. (6.) "The principle of multiple interpretations": If contradictory interpretations emerged, we tried to resolve this by going back to the data and check the context before discussing and agreeing upon an interpretation. This was performed in Braun and Clarke's phases 3, 4, 5 and 6. (7.) "The principle of suspicion": In order to avoid possible distortions arising from the narratives of the participants, we tried to design the semi-structured interview guide to focus on the area of interest as the main part (EDS) but as well as the context (information ecology) and clarify ambiguities during the interviews immediately. By combining the "local" EDS-view with the "global" contextual view, we reflected upon potential biases in the phases of analyzing and discussing the findings. This was performed in the phases 4, 5 and 6 proposed by Braun and Clarke.

Concerning the ecological validity of our findings, we follow the distinction made between representativeness and generalizability as the two components of the ecological validity (Kvavilashvili and Ellis 2004). Representativeness refers to the "naturalness" of a situation. We achieved this by asking the participants to have their EDS opened during their interview. Generalizability is obtained by taking into account the information ecology as described by the participants, and by contrasting this landscape with findings from our in-depth study focusing on the content of an EDS. During the interviews, we asked for clarifications when any ambiguous statements had been uttered, and we asked deepening questions so that the participants could elaborate upon their usage preferences and the distinctions they made concerning their choice of service. This understanding, taken together with our data-driven approach, gives us the confidence to have achieved generalizable findings. Especially, we did not have any pre-conceived assumptions that sharing in an EDS will or even must take place which is commonly associated with any cloud-based storage services. Therefore, we argue that the findings have been elaborated without theoretical distortion. The quotes in the following chapters have been translated by the first author when they originally had been uttered in German.

3.4 Findings

Our findings have been developed in a bottom-up and data-driven fashion. We first report on the type of content that is stored in an EDS before we report on the motivations why these information items were stored therein. Then, we present the context marked by other services that are used to store information items. Finally, we report on the curatorial challenges of going paperless.

3.4.1 Typology of Content Stored in an Electronic Data Safe

Comparing the three EDS services and the content people reported to store in an EDS, no big difference seems to exist with respect to the types of documents. We clustered the content types according to overarching topics based on their frequency and the importance attached to them as expressed by the interview participants. Two main categories of documents can be identified: "common" as the primary category and "selectively stored" as a secondary category. The reasons, why documents were kept, will be reported upon in the following chapter. The category of "common documents" is characterized by documents relating to an individual's financial status, official and physical existence, possessions, needs for protection, and being bound to legal duties. These categories have been utilized by nearly all participants. The second category of "selectively stored documents" refers to additionally stored items due to personal preferences. For an overview of the typology of documents, see Table 28.

Common documents	
existence	scans of passports, ID cards; licenses, birth certificate, excerpts of the crime register, official requests and decisions; rental contracts or purchasing contracts of real estate, statements of utility companies
finances	monthly statements, general banking-related items
possessions	receipts, invoices and warranty documents of "valuable" possessions
protection	documents issued by insurance companies
bound by legal obligations	tax-related documents, contracts (e.g. marriage contract)
Selectively stored documents	
managing other's data	family members and pets, persons taken care of as legal guardian
certificates and diploma	university/school diploma, certificates and other unique documents
health	insurance policies, general documents, health records, vaccinations
travel	reservations, booking references, passports etc.
(last) will and living will	last will and living will/advanced healthcare directive
leisure time activities	hobbies, activities in associations, membership certificates, tickets
invoices in general	keeping invoices from several companies or e-commerce activities
business-related documents	project data, invoices, offers, administration, customer data
miscellaneous	unspecified
private documents	personal letters, notes from parents
photos and videos	selected photos, e.g. photos from children's drawings, and videos
CV	for applications
mobility	documents related to the car or public transit
job related data	work contracts, schedules
archived data	former company, documents dealing with heritages, dissertation
legal entity	documents related to a private legal entity due to renting a house
subscribed services	inventory of subscribed services
access credentials	passwords, SIM card data, logins
Password safe	
account credentials	username, password
factual information	fashion sizes, PIN, software license keys, personal goals, tax IDs, for the owner and others (family members)

Table 28: Typology of documents stored in Electronic Data Safes

Common documents: Within the primary category of "common documents", we noted that nearly all the interviewees did scan their passports, ID cards or other documents that have been issued by official bodies to certify and document an individual's existence. These scanned ID documents were regarded as being very valuable and helpful, despite a scan lacking the legal qualities of the physical original. Official documents that were issued by authorities to prove a certain legal status, right or communicating a formal decision for an individual as a citizen were stored within most of the EDS of the participants. These documents relate to an individual as an official proof that it has been taken care of and that it has been registered with official administrative or governmental procedures. In the same cluster dealing with these "common" documents, everything related to living somewhere, either rented or in owned property, will be subsumed therein. This encompasses regular statements of utility companies as well as documents that justify the right to stay somewhere (rental contracts) or plans of the real estate.

Documents related to the financial life of a person were stored in an EDS by nearly every participant. Especially monthly statements and general banking documents were kept safe there, thus proving that someone has financial powers. In this cluster, documents related to retirement pension plans are stored. Documenting possession by digitizing receipts, invoices or warranty documents was performed by the largest part of our participants, too. The merits of existing and being financially potent to buy things of value entail a need to secure these possessions by documenting ownership. Furthermore, if something should happen, the documents in this cluster might help to exert warranty claims or to deal with insurance companies. Protecting oneself against the loss of possessions and against various risks entails safeguarding this kind of "protection credentials" which are forming part of this cluster. This also pertains to documents issued by insurance companies, such as contracts. Nearly half of the participants stored such documents in their EDS to have proof of the fact and the details on how their life is protected. Another cluster of documents is formed by legal documents binding someone to obligations imposed by law (taxes) or self-inflicted obligations due to entering

contractual, thus legally binding, relationships, be it business-wise or on an interpersonal level (for example, a marriage contract).

Selectively stored documents: In this category, several participants remarked that they are managing *other people's data* within their EDS. In most cases, one partner acted as the digital custodian of the partner's or family member's data, for instance, scans of ID cards. One interviewee mentioned that he stored all the documents related to his function as a legal guardian for several people in his EDS. *Health-related* documents, such as insurance policies or general documents issued by a health insurance company, were commonly referred to as belonging into an EDS; but they have not been mentioned so regularly compared to other kinds of protective contracts. Health records have only been stored by one person in an EDS whereas some more tried to keep their vaccination record up to date in an EDS. All documents on *traveling* enjoyed a wide acceptance and storage in an EDS. The main motive behind having such documents in an EDS was to be able to retrieve them in the case of need, maybe due to theft. Reservations and booking references, as well as copies of passports, etc., were commonly reported to be prepared in advance. *Other leisure-time activities* with a need for entrance tickets or general activities in associations or clubs also produced some documents that the participants wanted to keep safe in an EDS. Keeping and organizing *invoices* involves another category of documents. The breadth and depth of collecting invoices are highly individual. Participants noted that their personal schemes for organizing digital items are either thematically or pertinence-based. Still, a folder containing *miscellaneous items* often existed. Some of our participants are self-employed. For those, storing business-related data, maybe even containing *customer data and project data* as well as invoices or offers, an EDS was judged to be a suitable location for keeping such sensitive information items "in the cloud".

Although an EDS offers the potential to store every type of information, it was rarely used to store memorabilia, that means, items to evocate past events in future encounters. Only very few participants elaborated on "really private data", for instance, photos or videos, that they stored in an

EDS. Other categories that have been identified in the category of "selectively stored documents" are about *job applications* for which the current and previous versions of a CV have to be accessed and stored, *mobility-related* documents such as car leasing contracts or invoices from a garage. *Job-related data* was also kept in an EDS such as work contracts, schedules or locations of specific service points of a company that a mobile worker needed to access. Only a few participants explicitly named to have an *archive folder* where older data items, for example, from a former company the participant owned or a PhD-project, were stored for eternity. Another participant reported storing all document related to renting a property under the legal construct of a non-trading partnership with his siblings in his EDS which has to him an archival meaning. Other participants reported on storing information items about services they had subscribed to in an EDS.

Passwords: Besides storing documents or files, the dedicated password management functionality of the EDS services was used, too. Therein, surprisingly, not only passwords were stored. Our participants used it also to help to memorize PIN codes for mobile phones, tax identification numbers, membership numbers, notes, personal goals (as mantras), software license keys, factual information such as fashion sizes or the size of a mountain bike wheel. Some participants stored this not in the password safe but as regular documents. When participants estimated the number of passwords, their answers ranged from a few to more than 150 passwords (one participant used an encrypted spreadsheet file with more than 400 passwords).

3.4.2 Motivations for Storing Digitized Content in an EDS

In the interviews, the participants were asked to describe the character of the information items they store in their EDS. Furthermore, we asked why they digitized physical documents – regardless of where these information items have been stored afterward (see Table 29). The main motives are listed first.

In general, an EDS is considered as a *safeguarded digital home for sensitive data*. The participants expressed a huge variety what constitutes "sensitive" documents to them. For instance, financial statements were classified by some participants as very sensitive whereas other participants took a stance that such information is not so important. An EDS is also seen as a tool that helps in the transition from a physical to a digital filing system for general paper works, helping to *strive for the ultimate aim of having the paperless (home) office*.

motivations for storing content in an EDS	motivations for digitizing documents
safeguarding sensitive data	protection from loss
digital filing system/aspiring to the paperless office	aspiring to the paperless office
protection from loss	ubiquitous access
preserve long-term static data	greater accessibility
ubiquitous access	using in digital transactions
store everything and dynamic information items	saving physical space
reducing cognitive burden → passwords	digital copies help if a physical original is lost
	improves sharing capabilities

Table 29: Motivations for storing content in an EDS and for digitizing documents

Some interview participants reported that their only location for storing scanned and newly arriving documents is the EDS. Such a tendency to unify everything in one place (as the physical filing system had served this purpose before) highlights the desire to avoid information fragmentation ("[Scans of documents] are stored only in EDS service A. They still exist as paper. What would you recommend? If you do that [auth.: store them locally] then you will have stored things in parallel in 7000 locations again. But I think that the EDS service A should be sufficient.", A17). EDS services offer secure storage to *protect the stored information*

items from loss, especially for *long-term, static data* ("That are mainly documents that I consider to be important and that I do not like to disappear because of a fire or a flooding. If my house burned down, I need those documents.", B02 or "Documents stored in EDS service A have the potential to be needed sometime again in the future in order to look something up or for the taxes.", A02). This category was informed by the distinction the interviewees made between "dynamic" and ephemeral data and the preservation of "long-lasting, stable" information items such as digital copies of passports. Moreover, having ubiquitous access to one's data (every device, every place) was given as a motivation by only a few participants (5/39). And two participants thought of an EDS as a home for really everything digital they own; this also encompassed dynamically changing items, notably any files and documents that they create ("I thought, I will not make a difference anymore between storing documents in a safe and storing documents securely – in consequence, I will use [my EDS service B] for everything I am working actively with.", B16).

Each of the analyzed three EDS solutions gives the users the capability to store their passwords in the EDS which was actively used by 26 participants. Only service B offers an app that can be accessed offline to access the passwords. The main motivation for adding passwords to an EDS was to reduce the cognitive burden caused by the efforts to remember (ideally) individualized access credentials for each service. A centralized and seamlessly integrated access to their passwords has been reported by the interview participants to have positively improved their password management habits resulting in increased security.

Central motives of an EDS's usage are reflected by the motivations to digitize physical documents, too. The motives of "protecting from loss" and "aspiring to the paperless office" have been uttered equally prominently by the interview study participants. The motivations to digitize documents focus more on the beneficial affordances of digital information items such as their potential re-use in digital transactions. Albeit the motivation of having *ubiquitous access* is less prominently reported by EDS

users, they still see this as a huge motivation to digitize documents ("So, here is an example, you have got a confidential document like a driver's license that I now have got as a digital image in the cloud. Just in case I forget it, I could tell the police and show my driver's license as a picture.", B14). The dematerialization of information items as digital replica offers new affordances that overcome burdens associated with paper: digital information items are *more accessible*, for instance, by using full text search mechanisms ("I am massively faster compared to the time I had to look in folders through paper. Using the search function, I'm really faster now.", A12); they can be *used in digital transactions* ("I will add the [scanned] documents to certain business processes.", C02); they help *saving physical space* ("I had to reduce the space for document storage and folders by a third due to moving. When possible, I scanned and destroyed everything. I did this radically.", B08); they are *helpful in re-issuing physical documents* if they got lost ("Obviously, the [legal] value is not there. But if you have to redo your passport and lost it, or your passport gets stolen, usually they will ask you for a number.", B02); and they *improve the ability to share information items* easily.

When we asked the participants, what should not be stored in an EDS, half of the participants agreed that (almost) everything could be stored within such a service – if they trusted it. One participant – albeit using an EDS – mentioned that nothing should be kept in such a service because data would be given out of one's hands. In between these two extremes, the participants discerned two groups of information items that should not be stored in an EDS: high-impact and low-value data. As *high-impact data*, the participants thought of (a) financial data like balance statements, credit card data or – given as an example – documents confirming that they had been tax evaders, (b) information items that could be used to start transactions ("I would not save something in an EDS which could give access to other data. In case of doubt, I would not store the CIV code on the backside of my credit card." B10), (c) information items that could be used against oneself, and (d) various high-impact information items such as diaries, business-wise classified docu-

ments, contracts with attorneys, or documents related to the immigration in another country. As *low-value data*, the participants thought of saved journal articles, manuals, mundane invoices or own prose ("That would be everyday things. [...] A bill from the dentist, if it's not relevant for taxes, I surely will not upload it into EDS service A.", A11). Interestingly, multimedia information items (photos and videos) were explicitly exempted from belonging into an EDS by a few participants. The main reason given as an explanation was the lack of reasonably priced storage space provided by an EDS that would be needed for huge amounts of photos ("Pictures do not go in there because that would blow up the data volume.", B01).

3.4.3 A Still Life of an Information Ecology in the Presence of an EDS

EDS are used by the interview participants predominately for private purposes. Three out of the 39 participants used their EDS mainly for professional purposes, and all four self-employed participants mixed their private and professional information items in their EDS. To get a better understanding how this usage fits into the greater picture of other services used, we report on the "information ecology" of our participants in which other services are used, too. In doing so, we deliver a kind of differential diagnosis of the information ecology: the EDS vs. other services. The previous chapter depicted why an EDS is used through analyzing its content and the motivations of the users. In the discussion chapter, we will take all the information together to reflect upon the positioning of an EDS in the information ecology.

Google's services are used for private reasons by 21 of the 39 participants, whereas GoogleDrive was used by twelve interviewees. They reported that they used GoogleDrive mainly for saving and having a backup of photos, for instance, by using the automatic synchronization feature of their smartphones. The participants did judge GoogleDrive as a storage space for "unimportant" data that will be public afterward anyway or because they have no transactional value ("But this is all stuff that does not exert a higher level of privacy.", B12). Sharing and collaborating was also

the main emphasis how the participants described their main usage of GoogleDrive. Especially in the context of leisure time clubs (they were sharing out of print music scores), for students during their studies, or parents collaborating for school-related activities, GoogleDrive was preferred. Six participants explicitly stated not wanting to use GoogleDrive. GoogleDrive and GoogleDocs (formerly marketed as a separate product but now integrated into GoogleDrive) were seen as ideally complementing services because documents can be edited very easily, transgressing borders of devices, thereby eliminating the need for re-uploading an edited document.

Dropbox as a dedicated cloud storage service was used by individuals in a private context mainly for sharing photos (17 of the 39 participants) either with friends, family members, or for transferring documents. Automatic synchronization is used by five participants in order to keep several devices in sync or to have a backup in the cloud. In a professional context, Dropbox is used by five of the 39 interviewees. The main motivation reported by all interviewees was that Dropbox works seamlessly: it is available across devices and operating systems and offers a ubiquitous access to one's data. Moreover, this service is favored because it is the first one of its kind and, therefore, well known; due to its seamlessness, is judged as being easy, comfortable, and – very importantly – being free or modestly priced.

The participants also reflected on potential inhibitors of Dropbox's usage. The syncing client that has been viewed as a positive asset was judged by other users as an unwanted and aggressive way of uncontrollable data extraction out of their personal space of information into some far away location in the cloud. Other disadvantages were seen in the size limitation of the service or that job policies are forbidding its usage. The most compelling reasons for avoiding Dropbox was expressed by the participant's perception of their data stored in Dropbox having the character of being only a guest on a public space. The lack of encryption, the server location, and the company being domiciled in the U.S.A. evoked feelings of insecurity which especially became apparent for the interview

participants alongside the revelations surrounding the publication of NSA-activities by Edward Snowden (Verble 2014).

Nevertheless, the participants in the interview study frequently referred to as Dropbox being the gold standard when it comes to ease of use and seamlessness. To overcome security concerns, people shifted selected information items to other services (such as EDS service A and B), or only "unimportant" information items were stored there, like invitations, leisure-time related activities, cooking recipes or brochures. Still, backing up and synchronizing photos were used by 14 of the 39 participants; one participant added that only non-compromising pictures would be stored ("I mainly use Dropbox for private pictures, but not really private ones. If I share pictures via Dropbox or services alike, I do always question myself if I could cope with it when these pictures could be seen be someone else. If I am confident, I'll use Dropbox. Otherwise, I'll use encrypted e-mail or whatever else.", A13). Storing travel-related documents, scans of passports, or ID documents in Dropbox was also performed frequently – which was based on the ease of access if needed. Only one participant used Dropbox as his main storage for everything. Concerning "more private" data or "sensitive" data, six participants of the 39 participants in total stored valuable data in Dropbox which are: synchronizing their encrypted password manager file across devices, medical information of the daughter, a patient living will, invoices, job applications, pension plan documents, documents from others (parents, spouse), and some other "important" documents not described more closely.

Apple's iCloud-based services were used for private reasons by twelve out of the 39 participants. Five participants tried to consciously avoid these services because they felt a lack of control where their data was stored and had less trust in the company Apple or any company that has to follow the U.S. Patriot act. Five participants store documents or synchronize all their documents via the iCloud; eight participants used the iCloud to store their photos. The participants reported upon the reasons

for using the iCloud which are mainly based on the ease of use by synchronizing and having a backup at the same time in the cloud. Remarkably, one participant misused iBooks to store all her documents in there.

Microsoft's OneDrive is used by ten of the 39 participants in this study but usage reports are far less extensive, and this service seems not be as widely spread as other cloud storage services. It is mainly used within a professional or self-employed context (four participants); only two participants used it in their private context but only for "unimportant" documents ("OneDrive is for my documents that are not confidential or secret. If some hacker was there, I wouldn't care. There is no secret.", A20). One participant noted that he will move from OneDrive to EDS service B in the future because EDS service B seems more secure to him. Another frequent user in the business context said, he only puts selected content in OneDrive that is not so critical. The main argument why the participants got into contact with OneDrive is its bundling with Microsoft Office – and a feeling that it cannot be avoided ("I had to use OneDrive because it was kind of prescribed by Microsoft.", A15).

Evernote is another service that is used by five of the 39 participants in the private context and by one other participant in the professional context. The usage patterns encompass note taking (long and short term), backup reasons, tracking things, or Evernote containing the entire document archive (one participant; the information items do match the categories what the other users stored in their EDS, see chapter 3.4.1). Notes were the predominant content type, but also documents that needed to be accessed ubiquitously or providing access credentials were stored. One participant recorded his fashion sizes (collar size, jeans size) as notes. Again, having travel-related documents at hand just in case if something was needed was a usage pattern exhibited by three interviewees.

Other service providers: The following services are used only by one participant each. *Hubic* is used to synchronize data between devices and to share photos with family members. For multimedia content, partici-

pants also used *Facebook*, *Flickr*, *ImageInvent*, Deutsche Telekom's "*Mediacenter*" or *WeTransfer* to store and share larger amounts of data. *SugarSync* is used as an online backup of pictures by one participant which was favored by him because the syncing client can be configured to sync directories independently. *Wuala*, a cloud storage provider with client-side encryption, has been actively used by three participants during the time of the interviews. Seven other participants had used it temporarily before but abandoned. The main negative issues that were voiced by the interview participants were a complicated user-interface, a difficult handling of mobile up- and downloads, and the fact that the once free service became a paying one. As huge benefits for this service, the client-side encryption and being a Swiss service have been remarked by the interviewees repeatedly.

Running own servers: One interviewee reported that he is using his *own RAID* to store all of his data. Three participants administrated in former times an *own server running cloud services*. They reported having given up on this because regular maintenance became too time-consuming. Additionally, they argued that the benefit of resorting to professionally run services is the freedom from caring for everything yourself. Another participant even dismissed the general thought of self-administrating servers as too time-consuming – he just wants a tool that simply works.

3.4.4 Curatorial Challenges of Going Digital

This chapter reports on the challenges that our interview study participants experienced to maintain and keep their information items flowing in their information ecology.

Digitization of existing paper: A common challenge expressed by the interviewees was the initial effort that is necessary to put existing documents as scans into an EDS. Another challenge experienced by the interviewees was, what they should do with the physical original after scanning. Our participants expressed a tendency to keep "valuable" paper if it has legal value (with a signature or a stamp) considering these as *unique*

originals ("I am reluctant with my reference letter from my employer. If it is clear that I will need it electronically, I scan it. I would not destroy the original.", A07). On the contrary, *bulk items* (warranty certificates or receipts) maybe having a scanned signature (insurance policies) will be destroyed after scanning ("No, I did throw away the originals. So what? You can print them again anytime.", A12). Still, some participants expressed insecurity about the best approach in the future, leading them to keep, for instance, paper receipts to deal with warranty issues in the future. Another challenge was described by the participants with respect to retro-digitizing existing valuable documents. Unless they are not needed in electronic transactions, our interview participants judged this pro-active scanning as too laborious. Moreover, the interviewees suggested an "on demand" approach of digitizing when something old is needed ("I would digitize reference letters when I would need those.", A19). Some participants feared that paper-based information items will become inaccessible after their transition to a digital filing approach ("Starting September this year, everything new will be scanned; what exists before this date, I will leave it untouched. If I needed to digitize everything in retrospect, I would need to take two to three weeks of vacations.", A19).

Six of the 39 participants had a "digital only" strategy, that means, that they scanned everything which was a physical document: "I've got no paper folders, no envelopes. If it is important enough that I will keep it, it gets scanned." (B05) Or: "I do not like to make exceptions. If I go for electronic storage, then the full way." (B08). Notably, going fully digital seems to coincide with having the right scanning equipment which will serve as a catalyst. All the participants with a "digital only" strategy used a scanner with a document feeder: "Then I bought a new scanner. It has an automatic document feeder. Then, I thought, this is really fast – I can do this extensively. Now, once a month, I will process the paper. This is very fast." (B08) Some of these frequent-scanners expressed that scanning became an automated routine ("I have got such a multifunctional device with a duplex scanner built in. Over time, scanning became a routine.", B11). The scanning avant-garde of our participants expressed their favor for having a paperless office. Nevertheless, they mentioned some

challenges arising from this strategy: First, they have to remember to update content if new documents arrive physically ("And it is just a matter of keeping things updated. For instance, if I have got a new life insurance or a new insurance policy. I would have to think not to forget to put it into EDS service B.", B02). Second, if collaborators need to have access and are not using an EDS or prefer paper, something needs to be printed again ("As long as I am working alone, it is easier. Limits exist, for example, when my mother didn't have access anymore. She wants to have the documents that is why I suddenly need paper. I have to print it for my mother. It became more complicated through this.", B08). With relation to the information ecology as a metaphor, this is an ideal example of co-evolution: social or technological spheres repeat their evolution cycles in order to adapt to and benefit from changes in the environment.

Document providers are used implicitly as outsourced storage: Document providers or issuers, such as such as credit card or utility companies, are mostly companies in a B2C relationship with the document recipients. They will send documents to individuals by e-mail, the provider's specific portal or within an individual's e-banking portal where also the payment can be executed. Our participants showed four strategies to manage these information items sent to them: (a) let the documents be stored at the service provider (20/39), (b) download documents from a provider and store them using cloud storage services (15/39), (c) download documents from the provider and store them locally (14/39), and (d) download documents from a provider and store them locally and in the cloud (10/39). Preference for downloading was given to account statements or any other financial documents bearing relevance for the tax declaration.

The majority of our interviewees seem to have outsourced parts of their personal archive by taking a laissez-faire approach. The underlying assumption is that the individuals assume that the service provider will be responsible for taking care of these personal documents. In the extreme, a provider's portal is considered to be an eternally accessible archive – something that reflects the outsourced curation of a distinct collection.

This finding is underpinned by the judgments our participants expressed towards the question how long documents will be kept by the service provider. This revealed a broad spectrum of impressions: some participants (7/39) expected the service provider to archive the documents for eternity, some others (5/39) guessed that this will be not forever, and some others guessed that the limits might be in a period within half a year to three years (4/39). In contrast to these outsourcers by laissez-faire, we identified a loss-aware subgroup of interview participants that prefer downloading all documents. The main motivation was to have information items under one's own control because the provider might not store them forever or even delete something ("Yes, I want to have these things with me, for example, if the provider should change something. Maybe documents will only be kept two years by the provider. But I would be independent then. If I should need something and could not have access to it, that would be cumbersome.", B11).

We assume that an assessment of impact is made on how severe the loss of the documents or the loss of access to them would be ("For example, when I will contract for financing real estate involving a huge amount of money, it is not sufficient to keep it only at the bank for me to access it probably somewhen. Let's put it this way: I would like to have this proof still with me.", B12). Moreover, this impact-based assessment and the (un)intentional delegation of long-term storage can be interpreted as a coping strategy in face of an increasing information fragmentation: "I have come to the point of using too many cloud services, and it got confusing." (B13) Besides avoiding to download documents oneself, our participants expressed their desire to have all important documents at one centralized location – something that has been achieved before with physical documents and their grouping into folders in a home office.

Providing access to others: We observed an unexpected pattern of a "share everything" approach: Some participants shared their individual access credentials with their partners, including all passwords stored in the EDS. They had the notion of having one family account which is shared by persons all having the equal rights and reasons for accessing

the information items stored in there ("I have got nothing to protect against my family, my son has all my passwords. We are one family.", A20). Instead of relying on technology to control this information sharing, it was replaced by social trust, often justified to prepare for fatal incidents or reasons of convenience to having everything stored in one place. This revelation of access credentials reflects currently enacted sharing patterns prevalent in the family or marital relationships: "Of course, my wife has access using my username and password. We shared it. I have got not security concerns about this. You have to tell someone, of course, just in case something should happen." (A03). Documents related to the last will are also shared, sometimes by deliberately revealing all credentials during an EDS owner's lifetime – trusting that the recipient will not misuse them ("I gave him [my brother] access to my whole data safe and he gave me access to his because you potentially could die. I would have done this also with my tax lawyer but only in a restricted fashion.", A15).

3.5 Discussion

In the following chapters, we discuss the positioning of an EDS in an individual's information ecology. Based on our findings, we introduce the concept of "data value zones" as a sensitizing concept. We then reflect upon areas of challenge and tensions that seem to be inherent in cloud-based storage solutions that have a strong focus on personal information items that might become potentially shared information items.

3.5.1 The Role of an EDS in an Individual's Information Ecology

In order to answer our research question "*Which role does an EDS have in an individual's information ecology?"* we started by taking a look at the content stored in an EDS. Our typology revealed that an EDS is the primary home to "common" and "selectively stored" documents as well as transaction-permitting passwords. The nature of most of the documents can be described as digitized unique information items, such as

certificates or reference letters thus reflecting the information property of uniqueness suggested by Whittaker (2011). These documents were scanned voluntarily for their use in electronic transactions (as action-oriented information items, cf. Whittaker (2011)), or to prevent loss of "digital originals" or digitized content. Our participants expressed that these information items are of higher value to them. Therefore, we argue that the content in an EDS serves as a collection of selected, high-valued information items for which a conscious keeping decision has been taken. Only the participants who used the synchronization client to automatically upload all their documents and store these entirely within EDS service B did avoid the problem of assessing the value of documents. In their continuous usage of the EDS as a synchronization and backup tool, they followed a keep-all approach implicitly deferring the hard to take keeping decisions, something that has been reported to be common for the curation of personal information collections in both, the digital and analog world (Marshall 2008b; Whittaker 2011).

Temporal aspects of managing information items have been covered in the PIM literature mostly as a dimension for the retrieval (Jones and Bruce 2005). However, newer findings suggest that these temporal aspects are less prominent than other characteristics for re-finding documents (Xie et al. 2015). Nevertheless, our data suggests that there might be some overarching dimensions of information properties that describe the information elements stored in an EDS: informativeness, action-orientedness, uniqueness (cf. Whittaker 2011), and new: periodicity and subjectively assessed value. For example, statements of banks arrive on a regular basis and are archived by a user in an EDS due to their uniqueness (personalized information), their informativeness (current balance), and possible action-orientedness (for example, if fraudulent transactions are reported), therefore bearing a subjectively high value. These dimensions are overlapping, and their assessment might change over time due to external factors. This also makes it hard if not impossible to generalize, for example, a user journey or behavioral model with respect to the content types. For instance, banking statements might become a piece of evidence in the process of getting divorced to identify whom of the partners

contributed to which extent to their mutual income and wealth. Such a potential need for an unanticipated use also fosters the tendency to store everything and defer all the difficult keeping decisions. In the light of an unknown future, it is hard for individuals to decide which information items need to be kept based on some vague and dynamic characteristics. This also goes along with the ecology view which emphasizes the interdependent nature of the ecological system with its actors. Furthermore, such a fluid perspective is in line with the notion of a continuum thinking in archival science where records – or in this case information items – are "always in a process of becoming" (McKemmish & Piggot (1994), cited by McKemmish (2001, p. 334)) and are not strictly following a life-cycle with linear phases. Future research might identify further characteristics explaining these difficult keeping decisions.

It is an interesting observation, from a content perspective, that in the category of "selectively stored documents" the participants in our interview study managed information items for others. This indicates that "personal information management" becomes group information management within an EDS. Sometimes, this is done on purpose and with full consent, for example, the couple who decided that he will manage some parts of the electronic paperwork, and the spouse will take care of the other documents and the accounting. With respect to that insight, we even argue that an EDS can be interpreted as a transactive memory system (Wegner 1987): Each partner has his or her specialization, and they coordinate, for example, to organize and to retrieve documents for taxes, by resorting to a shared memory, the EDS. Both collaborators establish credibility in each other's capabilities of managing information items for a given task.

Protecting from loss was the main motive for using an EDS alongside with motives to get rid of paper documents to avoid a cluttered home. Therefore, an EDS serves as the centralized locus of curated, high-value information items needed in a long-term perspective. It can be characterized as a centralized, trusted repository uniting different digital assets from various origins – but, nevertheless, it is not the only service

in an individual's information ecology! This goes along findings in prior research (Marshall 2008b) that people will use several services due to various reasons and affordances despite speaking about their desire to have everything centralized in one place. Now, we can interpret this behavior in terms of an information ecology: a monoculture would provide short-term benefits but would be rather detrimental in the long run. When all access passwords are put into an EDS, it acts as a catalog of all digital belongings that are accumulated and distributed in an individual information ecology (something that has been suggested as an alternative to a centralized storage by Marshall 2008b). Storing multimedia data or sharing information items is organized via other services that seem more appropriate, for example, due to sophisticated functionalities or the fact that they are free of charge. Our participants used mainstream cloud storage services only for "unimportant" data when an EDS is present. The affordances of Dropbox as a seamlessly integrated tool into the operating system made it the predominant choice for sharing photos. When collaboration was needed, GoogleDrive was favored for editing documents. Microsoft's OneDrive was preferred in a business context. Our participants formed islands of collections, and they attributed special use cases or preferences to each distinct storage location. Generally, non-European service providers were often regarded as being less secure than European services which also is also reflected in the choice of services and the distribution of high-impact data in an EDS and low-valued and shareable data stored in non-European services.

3.5.2 Introducing Data Value Zones as a Sensitizing Concept

Our research question aims at identifying the role of an EDS in an individual's information ecology. Since our research approach is interpretive, we are now trying to reflect upon an EDS's positioning on a more abstract level, following the tradition of qualitative research to suggest new concepts that may be used to stipulate further discussion and research. All observations in our data provided us with a rich picture of the storage

locations and "information item valuables" that individuals are facing today. These findings indicate that different services are used to purposefully curate specific collections leaving us to wonder how they are interrelated. Based on the deliberate separation of services and the value judgments attached to the information objects, we conclude that different "data value zones" exist that guide the structure of one's PSI (see Figure 4). This concept is grounded in the thematic analysis of our interview data. It serves to illustrate overarching principles describing the perceived zones in an individual's information ecology.

We intend the "data value zones" to serve as a sensitizing concept for further reflections upon the levels where challenges in cloud-storage services might arise if they offer personal storage space that can be shared at the same time. The concept of the "data value zones" also draws upon the metaphor of the information ecology: The zones reflect the habitation (Nardi and O'Day 2000) that means the location of a technology within a network of relationships – from the individual to extended circles. Such circles of sharing and trust have been introduced in social networking services (SNS), for example, in Google+ (Kairam et al. 2012). This enables individuals to control which information items in SNS are shared with which type of audience and what facets (Farnham and Churchill 2011) of an individual are presented on the mediated "stage" of interpersonal communication (Goffman 1959). Our research thus extends this notion of sharing in SNS to any cloud storage services that individuals use to curate information items and possibly want or need to share them. The "data value" zones will be explained in the following.

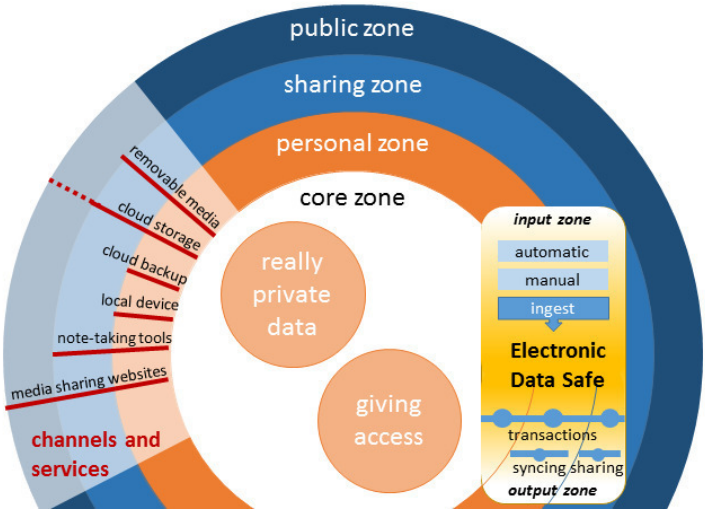

Figure 4: Data value zones

In an individual's core zone, the really private information items are stored, sometimes especially secured by encrypting them, for example with TrueCrypt. In this *core zone*, we place all credentials giving access to other services. Password managers might be used as a supporting tool, thereby implicitly creating an inventory of all digital services in use. The *personal zone* surrounds the core zone as the inmost circle. The content therein is regarded to be personal, either because it is directed from the outside to individuals or it is created by them. Since people are engaged in various social relations, sharing digital information items is performed in the *sharing zone*. Depending upon geographical dispersion, convenience reasons, or other needs, physical or digital storage solutions (cloud storage, SNS, etc.) are used to share items in a controlled zone – or at least giving the impression that the content transferred from the personal zone into the sharing zone is directed and equipped with implicit or explicit rules guiding the privacy of the transferred data to the other party involved. Finally, the *public zone* is dedicated to sharing in-

formation items with the general public as an audience for this broadcasting, for example, using media sharing sites or SNS. In the left part the "data value zones" illustration in the grayed area, the services and channels in a personal information ecology are depicted where sharing interactions take place. They may span several zones: for example, cloud storage services offer synchronization of personal data over devices and allow sharing. The previously identified categories of "common" or "selectively stored" documents are not bound to a certain value zone; their placement is bound to the context they are used within or their individually assigned value.

3.5.3 Creating Tensions by Spanning Zones Exemplified by an EDS

An EDS offers services that touch several "data value zones" which will be illustrated in the following. If an EDS's password management functionalities are used, the core zone is involved. An EDS can be used to manage information items in the personal zone and offers functionalities to share data in a (trusted) sharing zone. Furthermore, an EDS has an input zone which also spans the shared zone and the personal zone. Bearing in mind the concept of "data value zones", possibly problematic areas of tension might be identified when services in general touch multiple zones at the same time. For example, the participants in our study reported to be in favor of automatically receiving documents via their EDS; but at the same time, they expressed that these newly arrived documents should fit into their own, personal, organizational scheme which is effective in the personal zone. As we can observe, the transition between the sharing (B2C/G2C) zone into the personal zone could cause tensions. The output zone of an EDS is related to an EDS's capabilities of transferring information items to other zones. For example, synchronization clients might be used in order to securely share data from the personal zone with oneself crossing borders of devices.

If information items need to be shared with others or within electronic transactions, "data value zone" compatible sharing mechanisms are necessary to maintain "contextual integrity", a concept developed by

Nissenbaum (2010) and gaining momentum in HCI research (Barkhuus 2012): Privacy is not universally defined but individually granted depending upon the people involved, the content itself and the context in which the flow of information occurs. With respect to the "data value zones"-concept, this means that any spanning of zones must comply with the individually and context-bound principles to enforce "contextual integrity". To illustrate this, we refer to the subgroup of participants that downloads every information item. Although banking statements might be provided to them via their online banking portal belonging to the shared zone, they mistrust the durability of this sharing and try to bring this information closer to them by storing it in services or on devices that are belonging to the personal zone – which gives them the feeling of having everything under their own control. On the contrary, the laissez-faire types prefer leaving information items on the servers of their providers. Therefore, we conclude that for some collections, parts of the shared zone can be interpreted as an extension of the personal zone. Tensions arise if users experience that their intended placement of information items in zones is not matching the service's handling, for example, by deleting information items without prior notice thereby violating the "contextual integrity". The concept of "data value zones" helps to illustrate on which levels an EDS works and where challenges might arise. In the light of our observations, the tensions of concurrently sharing and safeguarding information items becomes evident in the context of an EDS. Another tension, which has been observed in the field due to transcending "data value zones", is related to an EDS's design for individuals but its shared use.

The tension between sharing and safeguarding, which was independently diagnosed in the recent work by Vertesi et al. (2016) can be confirmed by our observations, especially since our data is based on observations how people store subjectively identified high-value information items. Personal data is often judged to be highly valuable thus needing to be kept in a safe place, for example, an EDS. Nonetheless, people want to share or being able to access these information items in an easy way, for instance, when they are traveling and want to be prepared

for a potential loss of identity documents. An EDS should be safe and accessible at the same time. The same applies for documents concerning the last will or the patient will. Replicating the safe space, that means the personal zone, automatically with a synchronization client violates the notion of having something stored safely. In this case, the users' intention of having stored information items safely must be reconsidered since they watch them being distributed over devices. This causes worries: (a) information items might become accessible to someone else when a device is used by someone else, or (b) damaged information items, maybe due to a local virus infection, could be automatically synchronized thereby annihilating the once thought of safe space. These examples illustrate that conflicting needs exist. EDS service providers must creatively resolve this conflicting duality of safeguarding and needs of easy access. Providing mechanisms to control the flow of data to guarantee "contextual integrity" will be a challenge for EDS providers to avoid violating the "data value zones" individuals seem to have. Our work complements Vertesi et al.'s work by suggesting "data value zones" as locations where these tensions may occur and where interventions could be located that need to be designed to minimize or even avoid these tensions.

Further challenges with respect to transcending "data value zones" arise due to the primary design of EDS services being the secure storage location of choice for individuals which is challenged by the observed shared use. Family members were not granted access to an EDS using the "officially" designed functionalities, but they were given access by communicating the master key to the EDS. The same behavior was found in user studies on password sharing which observed that sharing with the family circle is an accepted strategy (Kaye 2011). Especially with regards to next of kin persons, an EDS was conceived as being the digital family archive or the digital equivalent of the paper folders stored in a location that was accessible to any of them. By opening up the whole EDS to others, the core, personal and partly shared "data value zones" are collated into one zone. This should be taken into account by generally all service providers offering person-bound storage services that a single-user design principle does not necessarily reflect actual usage patterns.

With respect to the information ecology concept, our "data value zones" contribute to a refinement and new insights characterizing the constituting elements of an information ecology: (a) system, (b) diversity, (c) coevolution, (d) keystone species, and (e) locality (Nardi and O'Day 2000). We will discuss every element in the following. (a) The *systems* forming part of an information ecology do have strong interrelations. If other services come up with new features (for example, encryption or data centers based in Europe/selectable locations), existing services need to adapt, or they might risk becoming an extinct species. Our findings have shown that users seem to thrive by using multiple services using them for specific tasks and certain facets of managing their information items. (b) The information fragmentation over several services with their specialization can be interpreted as a healthy *diversity* in an information ecosystem. This diversity helps to avoid unhealthy monocultures in the long run, for example by being dependent on only very few dominating players in the market. (c) Within the group of the "digital filers" that are using advanced scanning equipment, we were able to show that a *coevolution* of services, technologies, and social practices takes place: the whole ecosystem thrives if, for instance, digital filers are using the benefits of modern scanners which might, in turn, lead to further adaptation of technology and/or social practices. This observation highlights the usefulness of describing these activities as practices and understanding these as routines that are shaped and enacted by individuals while technological tools have been used for it or triggered usage. (d) Although being a risk in terms of a monoculture, the big players in the domain of cloud computing for private individuals can also be interpreted as keystone species. Without their efforts of providing ease of use for services and platforms, creating and sustaining demand for further service developments from the users or inhabitants of an ecology system would be slower or not existing. (e) Especially framing and understanding sharing decisions in an information ecology's *locality* as being based on "data value zones" helps service providers to optimize the design of technology in the habitation of PIM practices: As we have demonstrated in our findings, some PIM activities seem to be individual but are, in fact,

deeply rooted in social relationships, such as the caring for other family members' information items in one's individual PSI – without having functionalities at hand that take these social ties into account. Furthermore, we demonstrated that the concept of an "information ecology" based on the notion of "practice theory" helps to uncover practices that are shaped by individuals in their use of technology – and that are, in turn, shaping their practices as well.

3.6 Limitations

The presented research has been conducted mainly with participants in the Swiss context and a few international participants. Therefore, we assume there might be a cultural bias due to the socially transmitted virtues of being "well organized". Nevertheless, we argue that in explorative research such a bias is negligible. Participants are interacting in their information ecology with internationally rolled-out services and platforms, and we claim therefore that the experiences with an EDS's usage reflect recurrent notions towards safekeeping high-valued information items. For future research, approaching the cultural differences of "getting and being organized" might prove useful, nevertheless. Furthermore, being aware of our qualitative approach, we do not claim universal validity of our findings. Our contributions will help to uncover new problematic areas, which had been left otherwise as blind spots in the service design.

3.7 Conclusion

Our study portrayed the use of Electronic Data Safes (EDS). Starting from inside out by analyzing the actual content, the motivations of users and how other cloud-based services are used by them, we gained a deeper understanding how an EDS fits into an individual's information ecology and which practices are developed. This contributes and extends the literature on digital possessions in the context of personal information management (PIM). Our findings show that tensions exist if individuals are aspiring to go for a paperless PIM which entails challenges for practitioners and service providers: (a) assisting users to seamlessly

ingest information items to alleviate the problem of information fragmentation, (b) complying with the concurrent user needs to safeguard and share information items, and (c) dealing with a share-everything approach with family members or trusted peers resorting to social trust instead of technology mediation. These challenges need to be addressed by all the actors involved in document or service provision, such as cloud storage providers in general or providers for services that are part of an individual's information ecology. Our developed concept of "data value zones" helps to understand and locate problematic areas of friction that are relevant to all services that offer personal, secure data storage combined with data sharing capabilities. Such services touch the users' perception of data value and privacy, and they must bring additional value in an individual's information ecology by reducing frictions and information fragmentation.

4 The Challenges of Shaping a Digital Legacy in Presence of an EDS (Essay 3)

This essay is based on the following peer-reviewed conference paper:

Pfister, Joachim (2017): "'This will cause a lot of work.' – Coping with Transferring Files and Passwords as Part of a Personal Digital Legacy". In: Proceedings of 20th ACM Conference on Computer-Supported Cooperative Work and Social Computing. February 25- March 1 2017. Portland, Oregon, United States. DOI: 10.1145/2998181.2998262. In press.

Abstract

We present a qualitative interview study of 39 participants who describe their current practices and concerns with shaping a digital legacy, especially when they are using cloud-based storage services that unify secure file storage and password management functionalities in one service (electronic data safes). After introducing the transactional model of stress and coping as an analytical lens, we report on the users' coping strategies with respect to shaping and giving access to their digital legacy. Pre-mortem password sharing is identified as a common problem-focused coping strategy. Moreover, emotion-focused strategies of avoidance and ignorance are discussed. Challenges associated with passing on a digital legacy, such as the lack of enculturated practices, difficulties in the appraisal and selection of information items, the preference for deletion, and implicitly transferring data stewardship duties are described and discussed to develop design implications.

4.1 Introduction

There is an ongoing trend of delivering information items in a digital manner urging customers into going (in)voluntarily in the direction of a paperless home office. This does not only happen in the private sector but also in the public sector (Berger 2014). Eliminating paper has been heralded as advantageous for years but paper is still preferred in offices due to its physical affordances (Sellen and Harper 2002). Nevertheless, electronic document delivery in the B2B, B2G, and B2C domain is the main driver to substitute paper-based mail leading to a considerable decline in the volume of paper mail (Hildebrand 2015).

Platform-based and cloud-based services are increasingly used to manage the personal space of information. Electronic data safes (EDS, see chapter 1.6.4) are proposed as a technological solution to reduce the problem of information fragmentation (Bergman et al. 2006). EDS serve as a centralized, quasi-natural habitat for all important, digitally-born information items. These items can be, for example, passwords, electronic versions of insurance policies or statements from one's electronic banking. Any other digitized content, for example, construction plans of houses or passports (for a detailed description, see chapter 3), can be stored in an EDS as well in order to protect these information items from loss. EDS unite file storage and sharing capabilities as well as password management functionalities so that users can store any valuable information items in a single, secure location. In doing so, an EDS serves as the physical analogue of storing information items in folders, boxes, piles, safes, or strongboxes. What differentiates EDS services from other personal cloud storage services is their potential to be integrated into e-business and e-government processes in order to send, receive, and archive any "official" and thus potentially more valuable information items (Pfister and Schwabe 2015). The content of an EDS is not limited to such "official" documents: any individually assessed, highly valued information item can be stored in an EDS, for example, any audio-visual memorabilia like family videos or photos. In doing so, users benefit from an

EDS's professionally run storage infrastructure freeing them from the burdens to care themselves for data security. For example, users do not need to care for running backups regularly anymore if they take the leap of faith to store their personal information items in a cloud-based service. EDS are still an emerging technology in a very dynamic market of cloud storage offerings targeting private individuals.

The shift in the materiality of information items (from physical to digital) and through which channels they are delivered are assumed to change familiar and culturally enacted practices of personal information management (PIM). The channels are, for instance, e-mail, provider specific self-service portals, or electronic bill presentment and payment, for example, integrated in a bank's e-banking. All this happens during one's lifetime and impacts others as the recipients of digital remains in the form of a digital legacy or digital estate. This digital legacy is fragmented over devices, storage locations, and storage providers. At the moment, there are no existing institutionalized or enculturated practices that give guidance neither in shaping a digital legacy pre-mortem nor in caring for digital remains inherited post-mortem. This paper understands shaping a digital legacy as an individualized task with social implications. In our research, we focused on an individual's information items bearing an "official" character. These information items may have been received by or are needed in business or governmental processes to manage either an individual's or a family's administrative life. On the one hand, this entails maintaining bonds with organizations that are imposed on you and that originate from your rights and duties as a citizen, for example, to pay taxes. Or, on the other hand, there are voluntarily chosen bonds, for example, when you are doing business by investing money. Therefore, we consider shaping a digital legacy and inheriting digital items as collaborative processes with different stakeholders: on the one hand, there are the data owners themselves, and on the other hand, there are various stakeholders as recipients of a digital legacy based on their social or legal relationships with the data owner. Thus, data inheritance as a whole involves socio-technological practices that connect individuals through direct or indirect collaboration taking place either pre- or post-mortem.

This happens beyond the workplace in the private domain which is attracting an increasing number of research works in CSCW (Blomberg and Karasti 2013).

Our research is based on the assumption that the observed trend towards digital delivery of important information items could cause stress for the recipients and curators of a digital legacy because existing practices are not adjusted to the digital realm despite their growing importance. In Information Systems (IS) research, stress induced by the general use of or the adoption of information systems is researched under the term technostress. Existing research on technostress focusses mainly on the work-related sphere, whereas in the private sphere, technostress is still an emerging area of research (Maier 2014). Our research empirically identifies individual coping strategies related to shaping a digital legacy in the private domain where technology is used voluntarily. Taking such a socio-technological perspective, we will be able to uncover socially and technologically induced challenges that cause coping behavior. These observations will provide the foundation for design implications. Furthermore, existing research on information organization behavior, notably in the domain of PIM, will benefit from connecting exploratory observations to a well-established theory. In doing so, existing patterns and observations now become more explainable and at the same time, by resorting to a well-established framework, the design of interventions on a social or technological level becomes justified and grounded.

The contributions of this work are the following. First, we present current practices and challenges of users in their pursuit of shaping a digital legacy. Second, we derive design implications based upon our empirical findings. Third, we ground the prior, observationally derived PIM strategy of "benign neglect" in the well-established theory of the transactional model of stress and coping from psychology. This helps to strengthen research in the PIM domain which rarely offers a grounding of its findings in other theories and focusses more on the description of phenomena such as pilers and filers (Malone 1983), cleaners or keepers (Gwizdka 2004). Researchers and practitioners who are preoccupied

with the life-cycle orientation of data and users are the intended audiences of this work. Practitioners, for example, designers of digital legacy solutions that assist in preparing and managing one's "digital death" can benefit from our findings. Moreover, our work contributes theoretically to the growing body of literature related to a lifespan orientation in CSCW and Human Computer Interaction (HCI) with PIM as the particular domain of contribution. By focusing on users that have united or are trying to unite their valuable information items in an EDS, our findings provide generalizable insights into how files and passwords are handled as part of a digital legacy which has not been covered, to the best of our knowledge, in prior research.

4.2 Related Work

4.2.1 Research on Digital Legacies

In HCI, a turn towards a lifespan-oriented perspective (Massimi et al. 2011) on service design is ongoing. For example, Banks (2011) describes the current and future challenges of remembering physical and digital artifacts throughout a person's lifespan: from infancy, growing up, being an adult, then being a senior and finally experiencing a digital death. Thanatosensitivity (Massimi and Charise 2009) as a sensitizing concept was introduced to inform service design and analysis by either treating the dead as a subset of users who must be designed for or as extreme users creating implications for the living as well (Brubaker and Vertesi 2010). Dealing with the various forms of a digital legacy is a topic that is attracting increased research activities in HCI (Giaccardi 2011; Grimm and Chiasson 2014; Gulotta et al. 2013; Maciel and Pereira 2015; Waagstein 2014), CSCW (Brubaker 2013; Brubaker and Hayes 2011; Massimi et al. 2012), and it is also a topic that is covered in the public media (Jacobs n.d.). The term digital legacy is used quite vaguely in prior work and shall, in this work here, also imply that every information item digitally created and curated by an individual has the potential to become a digital heirloom given the right kind of socially-constructed circumstances (Banks et al. 2012; Odom, Banks, et al. 2012) once an individual passed away

(Carroll et al. 2010; Kaptelinin 2016). Such research on digital remains complements existing research on physical remains (Kaye et al. 2006; Kirk and Sellen 2010) to better understand how personal information collections are curated in an on- and offline world. Moreover, existing research related to digital legacies focusses very much on social network sites dealing with their role as a digital memorial (Acker and Brubaker 2014; Brubaker 2013; Brubaker and Vertesi 2010; Moncur and Kirk 2014). The problems of passing on digital items and managing a digital legacy have been analyzed from a legal perspective (Brucker-Kley et al. n.d.; Hopkins 2013), too. The file or password perspective has not been covered yet, to the best of our knowledge, even in a recently published categorization of systems supporting legacy-making, bereavement, and remembrance (Gulotta et al. 2016).

Technology-assisted mechanisms that support the handing over of a digital legacy have been developed in the last years. Widely-used commercial platforms have started to deploy their own solutions to deal with their user's digital legacy, for example, Google's "Inactive Account Manager" (Prates et al. 2015) or Facebook's "Legacy Contact Service" (Brubaker and Callison-Burch 2016). Starting much earlier, many startup companies have been flourishing in this market segment that is expected to grow with the increasing amount of life that is assisted by online activities. These service offerings range from (a) dedicated services for transferring accounts to beneficiaries (Peoples and Hetherington 2015), (b) posting memorial messages on social networks, to finally, (c) integrating password management and cloud storage in one service. Such a combination of a securely encrypted storage for files and passwords that is, at the same time, easily accessible as a cloud-based service, is realized within Electronic Data Safes (EDS) (Pfister and Schwabe 2013). An EDS serves as the equivalent of a physical safe where users can store any valuable information items – and eventually re-use them within e-government or e-business transactions based under the user-managed access paradigm (Pfister and Schwabe 2015). Thus, an EDS unites file storage and password manager in one service and offers either data sharing functionalities with general, multi-purpose sharing mechanisms and/or accompanied

by a mechanism for post-mortem, fine-grained data inheritance. To the best of our knowledge, no research was yet dedicated to investigate the role of an EDS in shaping or transferring a digital legacy.

4.2.2 Technostress, Stress, and Coping

Technostress, which is defined as an IT user's experience of stress when technology is used (Ragu-Nathan et al. 2008), has been researched in the IS domain predominately from a work perspective in which IT systems are used mandatorily as utilitarian artifacts in an organizational context (Maier 2014). Research on voluntary, hedonic use of IT artifacts in a private context, for example, using social networking sites as a source for technostress, is gaining initial research coverage (Maier 2014; Maier et al. 2012, 2014). As a theoretical foundation, research on technostress and interpreting the adoption of an IT artifact as a coping strategy (Beaudry and Pinsonneault 2005; Liu and Arnett 2000) is based predominately on the Transactional Model of Stress and Coping (TMSC) by Lazarus and Folkman (Lazarus and Folkman 1984) (Figure 1). It was also used as a theoretical lens to hypothesize about non-complaining despite negative incidents in the use of technology (Salo et al. 2015). In CSCW, this model has been used in qualitative research to identify coping strategies of remote team members (Koehne et al. 2012). In the following, a brief introduction will be given.

Stress can be the result of a person being confronted with environmental stimuli and their appraisal. Those stimuli are (a) life events such as death, divorce or life-threatening illnesses, (b) (natural) environmental events outside a person's control or (c) daily hassles that have a repeating occurrence (Lazarus and Folkman 1984, 1987). Being confronted with an event or a situation, a primary appraisal takes place. In this *primary appraisal*, the level of danger, the potential harm/loss or discomfort is evaluated by asking questions such as "How relevant is this situation to my needs? Or: "Is this situation congruent with my goals?" When no threat is perceived, no stress will be felt. Hence, the event or situation is considered as irrelevant. If a threat is identified in the primary appraisal, it will

be judged either as a challenge, a threat or a harm/loss. With the *secondary appraisal*, an individual assesses its potential for coping with the stressor. If own resources are judged as being inefficient, then stress results and coping strategies are developed. Coping is defined as "constantly changing cognitive and behavioral efforts to manage specific external and internal demands that are appraised as taxing or exceeding the resources of a person" (Lazarus and Folkman 1984, p. 141) And coping can take two general forms: the *emotion-focused coping* leads to an adaptation to the situation, the *problem-focused coping* motivates to take action and change one's situation. Furthermore, a *reappraisal* takes place in order to newly assess the situation under the chosen coping strategy (which is in itself a coping strategy). Despite its scarce usage in CSCW, the TMSC enjoys widespread usage in various domains, especially in psychology and the health sciences for researching coping with serious illnesses (Fredette 1995) or life events such as death and bereavement (Stein et al. 1997). Therefore, we based our research on the assumption that shaping a digital legacy could cause (techno)stress because this is related to a major life event such as death or bereavement. This will help to gain a deeper understanding of PIM practices which evolve from an individual to a social context when individuals shape or receive a digital legacy.

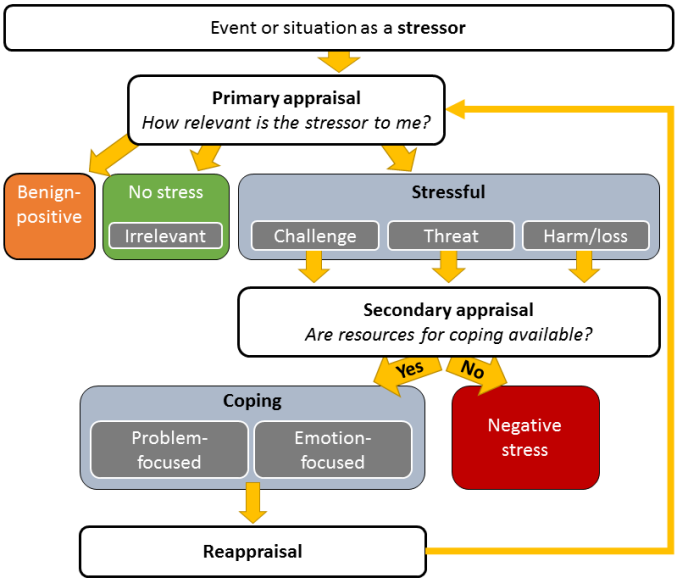

Figure 5: Transactional Model of Stress and Coping (TMSC), (adapted from Lazarus and Folkman 1984)

4.3 Research Design

We have chosen to follow a qualitative approach due to its suitability to uncover new phenomena and provide rich, context-specific information that may contribute to theory building afterward (Berg 2007; Venkatesh et al. 2013). In the following chapters, we first describe the empirical context and then report how the data collection and analysis was carried out.

4.3.1 Empirical Context

We used semi-structured interviews in order to collect data from 39 users of three EDS services. These interviews were carried out in a research project dealing with the current usage of an EDS and how it fits into an individual's information ecology (Pfister and Schwabe 2016). EDS services are promoted as the single home for digital valuables. Moreover,

they integrate document and password storage with functionalities for sharing and/or digital inheritance. Therefore, we assumed that EDS users were very concerned or thoughtful with their digital possessions if they chose to use such a service for managing their digital valuables. Three EDS service providers were contacted by the author and asked if they could give support in recruiting participants for an interview study. Two service providers are Swiss-based and are run by private companies (service A and B). The third EDS provider (service C) is part of the Austrian E-Government infrastructure and is run by a private sector company. The EDS service providers agreed to assist in the recruitment of participants only if they will be anonymized in any publication.

EDS service A is marketed as a safe location for storing documents and passwords to access them from everywhere. The service is offered for free. Files and passwords can be shared with other users of the same service using the service's all-purpose sharing functions based on folders and tags. *EDS service B* presents itself as a general purpose, secure online storage provider following a freemium pricing model. Besides storing files, a password safe is offered, too. Additionally, this service offers a digital inheritance functionality. The data owner can define which passwords or contents of the file safe will be made available automatically to a priori defined beneficiaries after the process of data inheritance has been initiated. It is started by entering a code that has been distributed by the data owner to the beneficiary pre-mortem. This code will unlock the selected information items after an individually defined grace period in which the data owner will be notified and could stop this process. *EDS service C* is provided as a data safe within the context of the Austrian e-government infrastructure. It is bundled with an e-identity component of a digital signature and has a freemium pricing model offering a safe space for storing documents as well as offering general data sharing capabilities, too.

The participants were recruited by self-selection and answering open calls for participation and they were offered a small gift. This resulted in 20 (EDS service A), 16 (EDS service B), and 3 participants (EDS service

C). The interviews were carried out via Skype, Google Hangout, or telephone except for two interviews which took place in the participants' homes due to geographical proximity.

4.3.2 Data Collection

We used a semi-structured interview guide that has been pre-tested. Its main focus was on the current usage of an EDS and which other services were used to store information items. In this part of the interview, participants focused on documents that were sent to them or that they received by participating in business transactions or with transactions needed to be carried out as citizens (for example, collect receipts for tax purposes). Therefore, participants were implicitly primed to talk about information items that had some business value to them in the broadest sense. In the last part of the interview, we initiated or deepened already given statements towards shaping a digital legacy: In particular, we asked: "*(1.) Did you ever consider what should happen to all your accumulated digital belongings that we were talking about during the previous part of the interview, for example, documents, accounts, photos, as your digital legacy? (2.) What feelings do these considerations cause? (3.) What items would you consider that shape your digital legacy? (4.) What have you already done or what would you like to do to take care of your digital legacy?"* All of the interviews were audio-recorded. In total, 39 interviews have been conducted (31 in German, 8 in English) resulting in 53 hours and 02 minutes of audio data. The author transcribed all the interviews. On average, the duration of an interview is 1 hour 19 minutes and encompasses a net number of 4079 words. Due to their self-selection, the participants had various backgrounds but they all had in common that they have chosen to use an EDS. 34 males and five females (for details see Table 27) took part with average age of 41 years (25-29: 4; 30-34: 6; 35-39: 3; 40-44: 7; 45-49: 7; 50-54: 6; 55-59: 3; 60-64: 3).

4.3.3 Data Analysis

After transcribing the interview recordings, thematic analysis (Braun and Clarke 2006) as a method for analyzing the interview data was applied.

This method has been successfully employed as an interpretive research paradigm in HCI (Vincent et al. 2014) and CSCW (Moncur et al. 2016) to systematically uncover themes. Thematic analysis is essentially a variant of the grounded theory approach (Glaser and Strauss 2009; A. L. Strauss and Corbin 1998) to produce themes instead of a full-fledged theory. The research in this study is conducted within a constructionist framework: The statements and observations are interpreted to uncover latent themes – to use the terminology of Braun and Clarke (2006). We proceeded inductively in a data-driven fashion without an a priori attempt to fit the data into theory. Relating our findings to the TMSC was done post-hoc, as described later.

In order to gain rigor, we followed the six phases described by Braun and Clarke (2006) which, in their essence, fulfill the criteria for qualitative research conducted in IS research as mentioned by Klein and Myers (1999). The interviews, as well as the transcription, were conducted by the author of this paper which allowed him to immerse deeply in the data by performing these steps himself and re-reading the data several times (phase 1: familiarize with the data). The analysis was assisted by using MAXQDA. Initial codes were assigned using open coding (phase 2). Axial coding was used to identify themes by collecting codes into potential themes (phase 3). Internal validity was assured by iterating between identified concepts and the assigned codes and themes several times, paying attention to reflect upon the researchers own perceptions and preconditions that might influence the research process (phase 4: reviewing themes). We did not opt for coding the data set independently by another researcher based on the understanding of coding as an active and reflexive process and that no exclusive reality in the data can be captured by assigning codes which would be more a realist assumption. An internal research report was written by the author which served as a means to define and name themes (phase 5 and phase 6). To increase internal and external validity, discussions with research peers proceeded to validate and refine the discovered themes. During these discussions, we noticed that the themes predominately dealt with strategies to overcome shortcomings in the current services and practices. This motivated us to search

for theories on coping to relate our findings to existing theories for explanation. We found several theories on coping in the domain of IS (Beaudry and Pinsonneault 2005; Liu and Arnett 2000) and became then aware of the discussion surrounding technostress (Maier 2014; Maier et al. 2012, 2014). We noticed that the generally accepted base theory of the TMSC has been used little in the context of CSCW (Koehne et al. 2012) and might be productive in framing the presentation of our findings and deriving implications for future service design, as well. In our analysis, we then proceeded by identifying which of our inductively derived findings match which elements and constructs in the TMSC.

The quotes in the following chapters have been translated by the author when they had been originally uttered in German. The brackets marking an interview quote indicate the EDS service's code (A-C) followed by the participant ID, and, separated by dashes, the participant's gender (m/f) and age.

4.4 Findings

When the interviewees were confronted with the questions related to a digital legacy, they first were a bit surprised – or spontaneously said: *"This will cause a lot of work."* (A01-F-59). Overall, the participants did not react in an uneasy way and it even seemed that they were curious and happy to share their experiences and concerns. In talking about this topic, the interviewees reflected upon their own practices and attitudes being almost thankful to have been brought to think about it (again): *"Yes, I have thought about this topic, but too little. That's really an issue. You pointed me towards it again. The more I use [EDS service A], the more I need to grant access to it for my wife or someone else." (A19-M-39)*

Only very few participants stored their last will or living will in an EDS. Most often, they referred to their whole EDS's content as being possibly relevant and becoming a digital legacy. For example, documents related to possessions (financial or property) as well as account credentials were thought of to become relevant for potential heirs.

4.4.1 Motivational Triggers

The main motivational triggers to think about issues related to one's own digital legacy were caused by experiences with death in the closer or wider circle of family, colleagues at work, friends, neighbors, or within virtual friends on social networks. For example, job-related encounters with death or bereavement caused some reflections: "Because I work in finance, I know how difficult it is to have access to money if no certificate of inheritance or other documents are available. In that case, I think it is important to give someone the access credentials for electronic banking services in order to settle something regardless if this is legal or not." (B01-M-44) Furthermore, EDS service B offers a digital inheritance functionality that, when it had been discovered by a few interview participants, triggered them to think about this topic ("When I saw it first, it came to my mind that this actually is a relevant topic. In the meantime, digital death became a mainstream topic: how to remove someone deceased from Facebook. When I started earlier, this was not a topic.", B15-M-49). Some other participants came to that topic because it was treated as part of their studies at university or due to their age and their considerations that nobody lives forever. Coverage in the media through articles in the press or TV or radio features on this topic was also identified as a trigger by a few interviewees.

4.4.2 Shaping one's Digital Legacy Put into the TMSC Context

The events that caused people to think about their own attitude or issues related to a digital legacy were mostly external events or stressors. On the contrary, an intrinsic motivation to actively take care of one's digital legacy was less often expressed and it was not necessarily bound to the participant's age. It often seemed that they felt an implicit obligation that their partner or family members should be entitled to have access to their digital legacy. Therefore, we conclude that besides internal or external motivational triggers other, culturally-induced stressors may exist such as a kind of moral or common sense-based code of "good conduct". These other stressors seem to reflect the natural order of inheriting something

and mirroring the expectations the participants are familiar with in the physical world. The role of the primary appraisal in the TMSC can be seen at work in the relevancy assessment of the stressor. For example, if no children are present, not having dealt with one's digital legacy was judged as being irrelevant thus no coping strategy needs to be developed – as observed within our participants that they have not taken huge efforts to transfer their information items as a digital legacy to their heirs or partners.

Creating or curating information items electronically were considered as a stressor by most of our participants. Especially photos were commonly referred to as being very valuable whereas other documents such as bank account statements were judged as less valuable. With reference to the TMSC, we argue that the type of documents influences how severe their loss would be assessed within the primary appraisal. In the following secondary appraisal, an individual assesses if existing resources are available. In our context, these resources are equivalent to strategies of transferring valuable documents, such as photos, to potential heirs. If such strategies are lacking, coping strategies are needed instead. The impact assessment is not only bound to death as a motivational stressor; other events such as potential accidents or being or becoming disabled can serve as a stressor, too. We also observed that appraisal decisions are context-dependent: if information items such as access credentials were used in a professional context, their potential loss was judged more severe than a loss in the private context. This gives rise to the assumption that each stressor (for example, private vs. business-related data) is assessed independently resulting in separate coping strategies.

4.4.3 Coping Strategies for Shaping a Digital Legacy

The observations in the interviews enabled us to identify four coping strategies when people are requested to ponder on shaping their digital legacy: (a) active caretaking, (b) avoiding, (c) ignoring, and (d) delegation to the service provider.

4.4.3.1 Active Caretaking

The majority of our interviewees are aware of themselves shaping a digital legacy and they did take some proactive measures to give access to their digital belongings during their lifetime or after their death. The strategies will be elaborated on in more detail in chapter 4.4.4.1. In taking preparations, the participants expressed their desire to enable the beneficiaries to act independently and "less burdened", alleviating them to follow the procedures dictated by the service providers, for example, to formally apply for access or deletion *("I wanted that someone could delete it actively without any problems and on his own – without needing to write a letter or to be dependent on the goodwill of the company if they will grant access or not.", B08-M-53)*. By having taken precautions, some participants felt that they complied with a moral demand to unburden the next of kin. Leaving behind or creating the need for accessing a digital legacy was seen by our interviewees not only in relation to death. They recognized and also identified other conditions. A distinction based on the severity was made with events that happened either surprisingly or developed gradually with death being the worst degree of severity followed gradually by other conditions such as accidents or becoming disabled.

Most of the participants described that account and access credentials should be part of a digital legacy in order to transfer control over them to someone trusted: *"I think this digital inheritance function is very important to me because the day I die, all these passwords and these accounts are open and I want someone to access them and maybe to shut them down or at least, to have control over them." (B02-M-44)* Less frequently, concrete document or file types were described as a digital legacy. Photos were the top-rated items that should be inherited due to sentimental reasons. Other multimedia contents, such as family videos or job-related videos were mentioned infrequently. Data stored on a mobile device was also considered as something to be passed on. Certain documents related to buying or renting property, health- or banking-related documents should be passed on, as well. One participant thought of the

whole of an EDS's contents as worthy to be transferred. Only very few participants noted that providing electronically access to important documents, such as the living will or the last will, must exist *("With regards to our patient wills, they need to be accessible.", B15-M-49).*

Nevertheless, just providing access credentials is seen only as a partial solution to the problem of digital inheritance: *"But then, I was thinking about it and thought that it is more complicated than to commit my wife my usernames and passwords or adding her information to my account. [...] I can't remember that we had a specific discussion about what we should do afterward with these accounts." (B09-M-47)* The beneficiaries will not necessarily know what to do with the inherited access credentials or data. The vast majority of our interview participants did not give any instructions what should be done with their accounts or data after their death. There was a feeling of implicitness that the partner or beneficiary would do the right thing: *"No, for what is obvious it is obvious, for example, what has to be closed is very clear." (A09-M-46)* or *"I've got the impression that my wife is very intelligent and that is why I would need to explain very little. She would know by herself what needs to be done." (A04-M-48).* Only very few participants provided some detailed information what should be done, especially in a professional context to provide clients with access to their business data.

4.4.3.2 Avoiding

Nearly a third of the interviewees reported on avoidance strategies to deal with issues surrounding a digital legacy. Even though some negative personal experiences occurred –for instance, the appearance of birthday reminders of deceased persons on social networks sites – this did not incentivize the members of this group to adjust their PIM practices with respect to a digital legacy. These triggers were not put into action because talking and thinking about death was interpreted as something causing unpleasant feelings *("I have not spent thoughts on this. Many things in my real life are far more important to me.", C03-W-41).* These uneasy

emotions lead to deferring any proactive measure which has been reported to have occurred with a few participants. Iconic for this feeling of unease and procrastinating is the following quote: *"I heard about this topic somewhere else. Then, I downloaded a checklist from the Internet which was four pages long. I read through them and thought: Well, I do not do this now. It is just too early for me.", B08-M-53*).

4.4.3.3 Ignoring

We noticed that people were aware of themselves shaping a digital legacy but they were not taking any precautions so far *("I thought about giving the password to my sister. But I have not done it yet.", A14-W-34)*. One other group of interviewees expressed that they have got nothing that they would need to pass on as a digital legacy. As one participant put it philosophically: *"The digital graveyard is just another graveyard of my existence." (C03-W-41)*. They do not see any reason to be bothered with the fate of their personal digital collections afterward: *"To be honest, I do not care what happens with my private photos. Someone shall do whatever they like to do with these." (A04-M-48)* If no children are present as heirs the question arose who would be interested in one's personal digital legacy *("Since we have not had children, this is not so important for others. These are only things that are relevant to my husband or me. I do not think that this collection is of any historic value.", A01-F-59).*

4.4.3.4 Delegating to the Service Provider

Very few of our participants argued that it should be the service provider's duty to care for designing a proper user-lifecycle. This group thinks that the issues of transferring a digital legacy is best dealt with "professionally" by the services themselves – given that they show awareness of this problem. Then, the participants in this group said, they would use such functions. Nevertheless, a digital legacy was commonly recognized as growing in importance and relevance in the future *"... because more and more data will be stored electronically. That has to be considered. And providers need to become active either by informing or educating users or by giving them solutions at hand." (B03-M-51)*

4.4.4 Challenges of Passing on a Digital Legacy

In the following, we will present five challenges that are related to passing on a digital legacy: (1.) providing access, (2.) intertwined information items for shared use, (3.) lack of enculturated practices, (4.) hardness of appraisal and selection, and (5.) preference for deletion.

4.4.4.1 Providing Access by Sharing Passwords

We identified six strategies to proactively provide access to a personal digital collection after one's death. These findings motivated us to propose challenge 1: sharing passwords to provide access to (parts of) a digital legacy is state-of-the-art.

Sharing passwords with the partner or family members during one's lifetime (strategy 1): This is performed in several ways by half of our participants. Most commonly, partners shared access credentials because they felt a moral imperative that sharing with the partner is the norm and in a partnership, there is no need to hide something because they consider themselves as one single and unified team: *"I'm very open with my wife, she has got all my passwords we have got no secrets." (B05-M-42).* In most cases, conveying access to passwords was also associated with the access credentials to someone's computer or laptop. It was not clearly stated by the participants if device access entails access to other services, for example, such as an EDS. Some participants acknowledge that this strategy might only give partial access to a subset of a personal information collection or leave it impossible to decide on a fine-grained level what to share with whom: *"The only way right now, we found, is that she has the passwords of my software applications and I have got the passwords of her software applications. So, if one of us two dies, we could log in. The point is, that is just a buffer solution. It's not the final solution because I should be able to state upfront, when I do die, I want this account to be accessible to this person. [...] But I think we are far, far away from this situation." (A09-M-46)* Besides the partner, next of kin were given passwords because being one family was considered as belonging to the same, inner circle of trust: *"What I've done now is that my wife and son*

have all the necessary information to access all the things in the cloud. I gave them a paper. They have everything. I try always to share a maximum with my family." (A20-M-54)

Shared account use (strategy 2): Instead of having individual accounts, some couples decided to only use one password safe together. This shared account use was seen as a logical step because everything else is already shared together and no need for separation is felt *("In theory [accounts should be separated,] yes, but in practice we share them. We share our electronic banking and our Dropbox. Otherwise, there would be redundancy, and we would need to use services twice." (B10-M-32).*

One partner acts as the access credential secretary (strategy 3): We observed that in some families or couples, each partner engaged in a specialization, for instance, being responsible for the digital information infrastructure. Thus, this partner was perceived as the couple's or family's natural secretary for keeping all the access credentials. If the number of passwords grows, password safes are often used in which credentials of several persons are then mixed up together.

Informing in a paper-only strategy (strategy 4): Sharing account credentials during one's lifetime is often performed physically by handing over a piece of paper to a trustee. For example, one participant shared a paper-based list of passwords that needs to be updated from time to time (which reminded the participant to do so after the interview).

Informing in a hybrid strategy (strategy 5): This hybrid approach involves handing a master password written on a paper to a trustee who then has access to a password safe to obtain full access. *"I solved it in that I gave my brother, who also has my last will, a letter. Within my last will, there is one letter with just one word with the username and password to [EDS service B]. He knows it because I've told him. This letter is sealed. He would not open it when it is not necessary. So, if something happened to me, he would open it and thus had access to all data." (B10-M-32)*

Informing in an electronic-only strategy (strategy 6): Access credentials can be shared only electronically, for example, as an encrypted Excel

file synchronized over devices. If an EDS offers the possibilities to share documents or passwords individually, only very few participants used this electronic method, for instance, sharing parts or even the whole EDS with the partner, the brother or the children. If an EDS offers a dedicated digital inheritance functionality, this was actually used only by few of the participants. The advantage of such a dedicated digital inheritance functionality was described by one participant as to prevent misuse: *"If I lock something and give the key to someone else, this person could unlock something when I am not there. You have to assess the risks how likely misuse will happen." (B12-M-33)*

4.4.4.2 Intertwined Information Items for Shared Use

Our participants identified several areas of problems that might arise when something is passed on. In the private context, they expect that some information items will still be needed because death does not necessarily terminate every legal bound automatically. Many of the stored information items, especially if one partner is doing the home office work on behalf of the other, are intertwined resulting in a mixture of individual data and mutually shared data that needs to be passed on as a whole. Moreover, one participant mentioned that in his files private and job-related documents are mixed, because he prefers using his personal file storage services than the company-provided "worse" ones. In case the participants were self-employed and they were using an EDS, they emphasized the value of their job-related information items stored in their EDS. Digital inheritance, in this case, is seen as a prerequisite to guarantee business continuity for the clients which has been imposed on them as part of their mandate. Therefore, we subsume all those observations by proposing design challenge 2: information items in an EDS have the potential to be used as shared resources.

4.4.4.3 Lack of Enculturated Practices

Dealing with a physical or monetary legacy, the participants perceived the processes surrounding this life-event as rather institutionalized and formalized so that they know what they would be expected to do or to

deliver *("Generally, we have taken precautions what has to be done then. But the digital side is still lacking.", B07-M-56)*. But passing on digital belongings is regarded as something new and challenging because no script-bound procedures exist. The main problem, as diagnosed by our interview participants, is to simply know about the existence of digital spaces where information items are located. For instance, partners or children do not necessarily know that maybe important documents are stored within an EDS *("Two of my three children would not even know what [EDS service A] is. And even with my third child, I did not talk about this topic. I assume that he knows that I am having an account there and that I have stored documents there.", A13-M-27)*. Another interviewee reported on the death of his work colleague and the problems of his wife: *"She had no clue what the password was. She did not even know where he had bank accounts.", A08-M-54)*. Besides this lack of general knowledge, other problematic areas were described, such as that the partner is not that tech-savvy or that the interviewees assumed a kind of responsibility of the data owner to take precautions with digital belongings upfront. However, they often described a feeling of unpreparedness or helplessness with this task. This indicates that recipients of a digital legacy are dependent on a direct or indirect collaboration with the (former) data owner to avoid that data inheritance fails when it is interpreted as a socio-technological practice. We summarize these findings by proposing design challenge 3: just inheriting access to act in the sense of the data owner might not be sufficient for beneficiaries of a digital legacy.

4.4.4.4 Hardness of Appraisal and Selection

Our interview participants assumed that the biggest challenge is to know what counts as one's digital possession and which parts of it should be selected to pass on. Some participants had the notion that besides a will or a patient's living will a kind of third will – the "digital will" – is needed to decide upon what happens with one's digital estate. For the passwords, the participants developed several strategies. However, they wondered if they should open up everything, or only provide limited access. This selection process, or to put it into the language of archivists, the appraisal

process to select important from less important documents, is regarded as a difficult decision. To summarize our findings, we propose design challenge 4: users find it difficult to decide which information items should be passed on.

4.4.4.5 Preference for Deletion

As one participant put it, there is often an ambiguity between the desire to leave traces and covering the tracks at the same time. In our data, our participants did express some general preference for having digital information items deleted or accounts closed. We noticed a kind of immanent desire to "tidy up" things. Deletion and deactivation were favored for social network sites but not necessarily for documents, files, especially photos, and e-mails: *"Facebook needs to be deleted. And someone should be responsible for stopping social media ties from continuing.", A10-M-64)*. With respect to this desire of having things deleted, some participants favored a selective approach, whereas some others expressed their conviction that everything should be deleted to terminate one's physical and digital existence entirely *("I would say, when the time comes and I would be able to, I would delete everything. I think nobody needs my job recommendation letter anymore – that can be deleted. Invoices can be deleted then. Delete – and, that's it." (B11-M-46)*. Some other participant took the stance that he has not prepared anything upfront which will result in an eternal storage of his digital remains *"... in the cloud until someone deletes them."* (A03-M-51). In summary, deleting information items is favored by our participants but not necessarily for everything. Thus, we propose as design challenge 5: provide mechanisms to delete information items selectively.

4.5 Discussion

In this chapter, we first analyze our findings using the TMSC as a lens to demonstrate its explaining powers for the observations we made in our interviews. Furthermore, based on our findings, we will derive design implications by relating them to prior research. We argue that the newly

identified design implications are valuable for dedicated EDS services, and on a more general level, also for any cloud-based storage solution that will eventually become a digital legacy. The design implications will be summarized in Table 30.

4.5.1 EDS-related Coping Strategies in the TMSC Context

Based on our findings, we identified four coping strategies in relation to the challenges of shaping a digital legacy. If users take proactive measures in order to provide access, we interpret this kind of behavior as the result of a primary appraisal causing a feeling of fear or loss. Within the secondary appraisal step, insufficient resources might be diagnosed that one is unable to always provide access to certain information items which will entail the coping strategy of "providing access". This is a problem-focused coping strategy because people are trying to change the problematic situation themselves by handing over passwords or engage in data sharing activities. With the TMSC in the background, we assume that password sharing is used as a problem-centric coping strategy to avoid leaving behind an inaccessible digital legacy. Password sharing is chosen as the easiest and most controllable (social trust instead of technology) first aid remedy since no other enculturated practices have been established for giving access to a digital legacy. We also identified two emotion-focused coping strategies: avoidance and ignorance leading to no proactive behavior. These strategies are not the result of a neutral assessment of the primary appraisal. Our participants were aware of potential problems associated with leaving and shaping a digital legacy. Since they lack effective resources, the interviewees developed emotion-focused coping strategies instead of problem-focused ones. For example, participants did that by relativizing their age using the argument: Thinking about death and loss at times that are not considered as "ripe enough" for such thoughts seems to create negative emotions that are put away by following an emotion-based coping strategy of *avoiding* these thoughts. Moreover, some other participants expressed to ignore issues related to shaping a digital legacy. They also knew about the problematic nature but they chose to *actively ignore any need for caring* – which we interpret as

a coping strategy to control negative emotions associated with this topic. Even the participants that were confronted with motivational triggers of death occurring in their closer circle of family and friends did not automatically expose a higher degree of preoccupation with this topic. They were sensitized to it but most of our participants were not motivated to act proactively. With the TMSC in the background, we interpret this as an individualized decision related to an emotion-focused coping strategy of avoiding or ignoring this topic. Finally, the delegation to the service provider, is a *hybrid coping strategy involving a problem-focused and emotion-based focus at the same time*. Our participants expressed that they would favor the service provider to come up with functionalities. This is the technical or problem-focused side. But by expressing this desire to have someone else provide the right tools and features for shaping a digital legacy, the participants do use an emotion-based coping strategy, at the same time. They defer large parts of their responsibility to the service provider thus freeing themselves from the emotional burden to take care of their digital legacy themselves. Other research in the IS literature suggested that both coping strategies can occur simultaneously or in intertwined chains (Salo et al. 2015).

In summary, we argue that the TMSC as an underlying theory has explanatory potential for users' technology adoption decisions with respect to curating a digital legacy. An EDS is located in the private domain and is used to store an individual's personal "private" and "official" information. Our qualitatively derived findings support the views expressed by IS-based research (Maier 2014; Maier et al. 2012, 2014) that technostress is also observable in the private and voluntary use of IT artifacts.

4.5.2 Deriving Design Implications from Design Challenges

In the following chapters, we discuss the identified design challenges in the light of related work to develop design implications. For a summary, see Table 30.

4.5.2.1 Challenge 1: Providing Access by Sharing Passwords

As reported in our findings, password sharing seems to be an accepted way of providing access in the context of a family or a partnership. An EDS used as a centralized storage location serves as the digital equivalent of the former folders that were accessible to everyone at home. By sharing access credentials of an EDS with others, an EDS enforced single-user design and thus individualized PIM becomes the well-known group information management (Lutters et al. 2007) again. Instead of relying on technology to grant permissions, access granting is replaced by social trust. We assume that this might cause future social and technological tensions due to the mismatch between the intended single-user paradigm and the observed practices in which password sharing is common.

Existing research on passwords does not focus on the fact that they are forming part of one's digital legacy. Other research work deals with password management strategies (not related to sharing) (Stobert and Biddle 2014, 2015), the role of password managers (Hayashi and Hong 2013) or the preference of online vs. offline tools (Ciampa et al. 2011). Password sharing is tentatively recognized as a common practice, either at home for accessing a family computer (Brush and Inkpen 2007; Egelman et al. 2008) or as sharing based on careful and context-specific decisions (Kaye 2011; Singh et al. 2007) and should not only be judged as a misbehavior of users. Recently, device and account sharing (Matthews et al. 2016) were researched leading to a taxonomy of six sharing types: borrowing, mutual use, setup, helping, broadcasting, and accidental. However, no prior work explored how people share passwords in the context of shaping a digital legacy or how sharing actually takes place and which channels or media are involved. Our work thus supports and extends prior findings by identifying and describing six proactive strategies for password sharing in order to provide access to one's digital legacy. These practices show that an EDS's dedicated sharing capabilities are not necessarily used to achieve this goal or that they are even avoided.

As design implications, we suggest that EDS service providers need to offer functionalities that match current user practices as reflected by the

identified coping strategies of "providing access". This also applies to any cloud-based storage services that potentially will become a digital legacy. In the following, we suggest some design implications in relation to the uncovered password sharing strategies. Ideally, these implications help to develop design interventions. First, they should help to raise awareness of the problems associated with shaping and transferring a digital legacy so that the user's primary appraisal results in a judgment of relevance and not ignorance. Second, these design interventions need to provide resources or functionalities for users that they can experience competency in choosing and performing a coping strategy, for example by designating specific information items that shall be destroyed or passed on.

Shared passwords (strategy 1) are a sign of trust and a potential risk. We suggest that sharing and controlling must be made more usable for a data owner to check what is shared with whom. The transitional character of social relationships needs to be taken into account since relationships potentially might break up which entails consequences for once shared data or accounts (Moncur et al. 2016). This goes along with our finding that accounts are often used as shared accounts (strategy 2): Service providers should reconsider if their single-user design appropriately supports the transitions of social relationships that are undergone by users during their lifetime. That means, for example, that default sharing zones with family or partners as trustees might be pre-configured and that common social practices such as joining or leaving a group need to be addressed and supported by a service's functionalities. Moreover, we observed that one partner acts as the secretary of the family's or couple's access credential collections (strategy 3). As design considerations, we suggest mechanisms that help to indicate which information items are administrated on behalf of others or are shared ("mutual use" in the taxonomy of (Matthews et al. 2016)). In order to provide access to their digital legacy, some users preferred writing down passwords on paper (strategy 4). The affordances of paper are the benefits and weaknesses of this strategy at the same time: though it is very easy to write down access credentials, this creates potential security risks and fails if users forget to

carefully update entries that may have been seized long time ago. This problem of updating changes and bearing a potential security risk is also inherent if users convey their master password for an electronic password management solution via a paper-based medium (strategy 5). We assume, that in an electronic-only manner (strategy 6) using a centralized location for all account data will prevent these maintenance issues. We, therefore, suggest as design considerations that maintenance mechanisms are developed which help the users in keeping their inventory of digital belongings updated.

4.5.2.2 Challenge 2: Intertwined Information Items for Shared Use

We argue that the curation of information items in an EDS as a centralized repository needs to be supported by functionalities that are in line with social practices and connotations that have been diagnosed in prior research dealing with sharing (digital) possessions (Gruning and Lindley 2016) at home. In their work, Gruning and Lindley developed a new spectrum of (digital) ownership, in which some digital possessions are considered as shared resources, such as family computers or movie streaming accounts. These mutually shared resources implicitly compel users to act in a trustworthy and accountable manner. Our findings show that an EDS's content is not necessarily restricted to information items belonging to a single person. We observed that information items are often curated on behalf of someone else and that they might be considered as shared resources. These shared resources just happen to be administrated by the owner of an EDS who has been implicitly awarded this job of an "information item manager" in a family or relationship context. Thus, an EDS needs to be interpreted as a storage location for personal information items and, at the same time, information items that have a shared use and which are curated collaboratively by sharing account credentials. As design implications for an EDS, we, therefore, suggest that zones of default sharing for mutually used resources are established and made easily accessible and inheritable. We also think that this shared zone should not be automatically cut off if the account of the primary account holder becomes a digital legacy. Instead, the information items

with the mutual use connotation need to be identified and passed on separately.

4.5.2.3 Challenge 3: Lack of Enculturated Practices

We proclaim that just providing access to a digital legacy is not enough to solve issues related to digital inheritance. Brubaker and Callison-Burch (Brubaker and Callison-Burch 2016) identify and define three approaches to post-mortem data management which originated in the domain of social networks: (a) configuration, (b) inheritance, and (c) stewardship. If users engage during their lifetime (pre-mortem) in decisions surrounding the fate of their digital belongings, this was described as *configuration*. When ownership and control are transferred to an heir, for example by giving the heir the password in the last will, this is described as *inheritance*. As a third approach, *stewardship* is proposed which considers a designated person as responsible for data management. However, this person must further take into account the context of the social relationships.

Based on our findings and using the terminology of Brubaker and Callison-Burch (Brubaker and Callison-Burch 2016), we observed that access to the entire digital legacy, not only social networks, was provided mostly by using inheritance as a strategy and to a lesser extent configuration, for instance, by activating the digital inheritance functionalities offered by EDS service provider B. But the lack of instructions what the beneficiaries of the information items should do with them in general or with certain accounts in particular, is often left open. We interpret this kind of behavior as putting someone implicitly in the role of a data steward. This person is entrusted to act as a steward of the information items stored in an EDS in the sense of the data owner by having received the access credentials. Together with having been granted access to the data and accounts, this implicit data steward is thought of to respect existing social or legal bonds when dealing with the digital legacy. We acknowledge that access needs to be provided somehow. However, we argue that tension potentially arises if the beneficiaries are putting heirs of a digital legacy in the

role of implicit data stewards without having given them any instructional or technological support to act in the data owner's sense. Therefore, we suggest design implications to help the recipients of a digital legacy to act in the sense of the former owner. For example, information items to be passed on could be characterized and accompanied with a description explaining what to do with this category.

4.5.2.4 Challenge 4: Hardness of Appraisal and Selection

The tremendous growth of data storage as well as an increase in already digital born data sources are reinforcing the tendency to keep everything and, therefore, defer difficult keeping-decisions (Marshall 2011; Marshall et al. 2007). Generally, personal information items are stored with the attitude of "benign neglect" ignoring the consequences or needs of data management through deferral to somewhere in the future (Marshall 2007, 2008b). Bearing in mind the TMSC, we can now understand the psychological mechanism behind this "benign neglect": If no harm or no potential danger of losing information items is diagnosed in the primary appraisal, no coping mechanism must be followed. If the primary appraisal gave way to a secondary appraisal and an individual would not have adequate resources to deal with issues surrounding a digital legacy, then coping strategies such as a reappraisal and concluding that there is no problem might take place which serves as a justification to leave everything as it is – which reflects the notion of "benign neglect" as a laissez-faire coping strategy. Identifying this underlying mechanism opens up design implications for EDS services to overcome the user's tendency to surrender to this "benign neglect" and bringing them to actively selecting what should be passed on or not. For example, EDS services could try to give meaningful suggestions which information items might be "more valuable" than others because they might be mutually used or have a certain degree of uniqueness. If users would store their entire digital information items in an EDS, this guidance could relieve them from the cognitive burden to take these decisions without "knowledgeable" support. For example, scans of unique documents or digitized children's drawings could be assigned a different storage strategy (long term), whereas more

mundane documents, such as automatically received bank statements, receive a suggestion for automatic deletion after a certain period of time.

4.5.2.5 Challenge 5: Preference for Selective Deletion

Prior work of Grimm and Chiasson (Grimm and Chiasson 2014) used a questionnaire to ask 400 participants acquired via crowd-sourcing platforms about their preferences related to shaping a digital legacy, or – as they called it – leaving digital footprints. Their participants expressed a favor for deletion and handing over things to the next of kin. This goes in line with our findings that a large portion of our interview study participants favored the deletion of accounts after their death and having the next of kin given access to their data. We observed the same in our data, that social media accounts were more thought of as something that needs to be deleted and files – especially pictures – should be transferred to others. As design implications, we, therefore, suggest that the owners of an EDS should be supported to designate the information items which are to be destroyed, to be deleted, or to be passed on to others. For example, if an EDS provides password management capabilities, the EDS owner might decide to have his social media accounts deleted, whereas "official" accounts with utility companies will be transferred to someone else's care. With respect to information items, such as files (photos, documents, etc.), owners of an EDS might also selectively decide which items should be transferred in which contexts.

1. Providing Access by Sharing Passwords		
(a)	**DC:**	Shared password usage.
	DI:	▪ Sharing and controlling information items must be made more usable. ▪ Transitional character of social relationships must be taken into account for shared information items.
(b)	**DC:**	Shared account usage.
	DI:	▪ Reconsider the single-user design paradigm as a design principle. ▪ Introduce default/pre-configured sharing zones with family members or partners. ▪ Provide functionalities that match the social practices of joining or leaving such a zone of trust.
(c)	**DC:**	One partner acts as the secretary of information items or accounts for both of them/for others.
	DI:	Add functionalities to discern information items that are administrated on behalf of others.
(d)	**DC:**	Sharing passwords using paper and keeping passwords updated.
	DI:	▪ Make updates to passwords less burdensome, for example, by automating updates or adding reminders. ▪ Provide functionalities that the beneficiary of a master password for a password manager retains access in case of changes of the master password.
2. Intertwined Information Items for Shared Use		
(a)	**DC:**	An EDS contains personal information items and information items curated on behalf of others.
	DI:	▪ Introduce default sharing zones in order recognize these information items as jointly used resources. ▪ Access to information items for mutual use should not be cut off when the primary account holder dies.

3. Lack of Enculturated Practices		
	DC:	Beneficiaries of a digital legacy are put implicitly in the role of data stewards without sufficient knowledge what they should do with the inherited information items.
	DI:	Provide support to the recipients of a digital legacy to act in the sense of the former data owner, such as an indication which information items should be passed on or which ones should be destroyed.
4. Hardness of Appraisal and Selection		
(a)	**DC:**	Difficult keeping decisions are deferred and an attitude of "benign neglect" prevails.
	DI:	▪ Use the TMSC to identify possibilities for interventions to overcome a primary appraisal of "not relevant". ▪ An EDS might provide suggestions which information items are "more meaningful".
5. Preference for Selective Deletion		
(b)	**DC:**	There seems to be a preference for the deletion of (social media) accounts but less for pictures.
	DI:	Provide functionalities to designate which information items should be passed on or should be destroyed.

Table 30: Summary of Design Challenges (DC) and suggested Design Interventions (DI)

4.6 Limitations

The presented research has been conducted mainly with participants in the Swiss context and a few international participants. Therefore, we assume there might be a cultural bias due to the culturally enacted values of being "well organized". Nevertheless, we argue that for this kind of explorative research this bias is negligible and that other qualitative research in the PIM domain did also not strive for a culturally balanced set

of interview participants. For future research, approaching the cultural differences of "getting and being organized" might prove useful. Furthermore, we do not claim universal validity of our findings and recognize their origin bound to a certain context within a user-study related to EDS services. Nevertheless, as such services mirror general functionalities offered by mainstream cloud storage services, we assume that our conclusions are transferable to other contexts and services that are used to shape a digital legacy.

4.7 Conclusion

Engaging with digital tools and services creates traces and information items which will sum up to a digital legacy that will be dealt with by the users themselves pre-mortem or by others post-mortem. In the authors' understanding, shaping a digital legacy constitutes a socio-technological practice: the data owners and various beneficiaries as stakeholders are involved in a direct or indirect collaboration to transfer or to receive digital information items as part of a legacy. Our research contributes to understanding how users are shaping their digital legacy, especially if they are using a dedicated, centralized, and cloud-based storage location for their valuable information items that, in our study, has been implemented in an electronic data safe (EDS). Our findings also confirm that technostress is present in the private domain for voluntarily chosen interactions with information systems, for example, by shaping a digital legacy with the help of an EDS. Furthermore, we were able to show how the technostress' underlying theoretical foundation, the transactional model of stress and coping (TMSC), can be used productively as an analytical lens. Additionally, we have demonstrated that this foundational theory is useful for explaining how "benign neglect" works, thereby grounding an establish observation of a phenomenon in personal information management (PIM) with a well-establish theory. This helps us to interpret current practices of shaping a digital legacy as coping strategies and to identify contact points for interventions based on a well-founded theoretical background. We introduced "providing access" as a problem-

based coping strategy. In this respect, we were surprised about the expressed strategies for password sharing that are used to give access to one's accumulated digital information items without using the EDS's providers' functionalities for data sharing or digital inheritance. We confirmed prior research for a preference on deletion as well as an implicit desire to have someone act as a steward of the digital legacy instead of just inheriting access.

As we have seen, several challenges exist for practitioners that create services to assist in shaping and transferring a digital legacy. Further research is needed to uncover other problems with respect to thanatosensitive design. Password managers as well as combined solutions of password managers and secure file storage, such as implemented in an EDS, have the potential to become essential components in a lifespan-oriented PIM. Marshall (Marshall 2008b) proposed to create a catalog of an individual's digital belongings instead of centralizing the storage of everything in one place which will undermine the user's notion of using specialized services for certain tasks. This idea originated in the context of personal archiving but its considerations hold for EDS services, too: By uniting secure storage of files and passwords, they will serve, at the same time, as an archive and as catalog where all other resources and information items are located. If a digital legacy needs to be shaped or transferred, such a collection of individually curated, highly-valuable information items and a catalog of accounts (that means, the password management component) could be very useful if digitization in the private homes continues. Nevertheless, these services need to take into account current cultural and legal practices to design functionalities that will be beneficial to the users. Our work gives initial design considerations that can be used either by EDS services or other cloud-based storage solutions providers which also have the potential to become a digital legacy. Another huge challenge constitutes in the need for an enculturation of these practices of shaping and transferring a digital legacy. We think that the service providers need to come up with solutions and give the users guidance as well as initially helping them to get awareness of this topic so that it will become an integral part of one's digital journey of life. Our research

findings and design implications will hopefully contribute to this so that users are not totally appalled when they think about their digital legacy urging them to say: *"This will cause a lot of work."* (A01-F-59).

5 Active EDS and Transformational Government – Evaluation of a Prototype (Essay 4)

This chapter is based on the following peer-review conference paper and has been extended[25]:

Pfister, Joachim and Schwabe, Gerhard (2015): „Electronic Data Safes as an Infrastructure for Transformational Government? A Case Study". In: Tambouris, Efthimios; Janssen, Marijn; Scholl, Hans Jochen; Wimmer, Maria; Tarabanis, Konstantinos; Gascó, Mila; Klievink, Bram; Lindgren, Ida; Parycek, Peter (Eds.) Electronic Government, 14th IFIP WG 8.5 International Conference, EGOV 2015. Thessaloniki, Greece. Proceedings. Springer International Publishing, Cham. pp. 246–257, DOI: 10.1007/978-3-319-22479-4_19.

Abstract

This essay introduces and explores the potential of an active electronic data safe (AEDS) serving as an infrastructure to achieve transformational government. An AEDS connects individuals and organizations from the private and the public sector to exchange information items related to business processes following the user-managed access paradigm. To realize the transformational government's vision of user-centricity, fundamental changes in the service provision and collaboration of public and private sector organizations are needed. Findings of a user study with a prototype of an AEDS are used to identify four barriers for the adoption

[25] This essay has been extended using yet unpublished research findings originating from the evaluation of the AEDS prototype (chapter 5.4). These new findings contribute to a deeper understanding what users expect of an AEDS and give insights for future service design which are suggested as design implications in chapter 5.6. These findings were also integrated into the essay's discussion.

of an AEDS in the light of transformational government: (1.) offering citizens unfamiliar services having the character of experience-goods; (2.) failing to fulfil common service expectations of the customers; (3.) failing to establish contextual integrity for data sharing, and (4.) failing to establish and run an AEDS as a multi-sided platform providing an attractive business model. Furthermore, with the help of this explorative user study, new potential benefits and challenges are identified. They help to expand our understanding of the potentials and problematic areas of an AEDS. Design implications are suggested to address these challenges.

5.1 Introduction

In many countries, electronic government (e-government) initiatives have been introduced that are progressing from the stage of information provisioning and simple transactions to more customer-centric stages of integrated service delivery (Veenstra et al. 2011). Several e-government maturity models and e-government definitions have been proposed (Yildiz 2007) but, actually, many e-government initiatives resulted in digitizing existing practices and were not able to reach more mature stages. In recent years, the idea of "transformational government" (t-government) gained momentum which is defined as "[...] the ICT-enabled operations, internal and external processes and structures to enable the realization of services that meet public-sector objectives such as efficiency, transparency, accountability and citizen centricity." (Weerakkody et al. 2011) The realization of t-government entails fundamental changes in the public service sector's practices and structures, for instance organizations need to cooperate and integrate their activities (Dhillon et al. 2008). This means to overcome data silos, take a holistic view on the relationships between the public sector and citizens or private sector stakeholders and to empower the citizens (CS Transform 2010). This results in a more efficient service delivery and a more transparent and responsive government (Veenstra et al. 2011). In this paper, the concept of active electronic data safes (AEDS, see chapter 1.6.4) as an infrastructure to support t-government is introduced and will be explored empirically. These AEDS are based on the paradigm of user-managed access, i.e. that an individual decides which information items are shared with an organization. Using the genre of a case study, a prototypical implementation of an AEDS connecting citizens, the public administration and private sector companies will be analyzed. This concept of user-managed access put into practice will be used to identify challenges with respect to t-government. Therefore, the research question of this essay is: *What are the challenges and potential benefits with respect to t-government when the concept of user-managed access with an AEDS is put into practice?*

The aim of this essay is to identify challenges for solutions supporting t-government that follow the paradigm of user-managed access based on a user study with ordinary citizens. Such an approach helps to complement existing literature-based approaches. For electronic data safes, to the best of our knowledge, no evaluation exists helping to identify this new class of tool's implementation challenges. Heath et al. (Heath et al. 2013) describe evaluation results from an AEDS-like tool but not with a focus on user perceptions. And research concerning the adoption of an electronic postal service, which also goes into the direction of an AEDS, has been carried out by Berger and Hertzum (2014), but they are focusing more on the challenges of the organizational introduction.

Existing research on the adoption of t-government and the identification of potential barriers to t-government is performed on a very high level such as analyzing the policies of national governments to assess their t-government readiness (Parisopoulos et al. 2014). Other research contributions use case studies in which they interview experts that are responsible for designing and running e-government services (Dhillon et al. 2008; Veenstra et al. 2011). Moreover, technological solutions that support t-government's service delivery are also researched: For example a platform-based approach (Bharosa et al. 2013; Janssen and Estevez 2013) to exchange data is discussed but only from a G2B perspective and with a focus on platform governance and information infrastructure. Hence, in existing research with respect to t-government, the individual as a citizen is rather put aside although user-centricity is a widely-heralded tenet of t-government. We argue that a thorough understanding of the socio-technological issues is needed before services are designed. A deeper understanding of the citizens' needs and preferences contributes to successful service design which will entail adoption by the citizens. This point of view has been recognized in IS research (Brenner et al. 2014) and needs to be embraced in the t-government context, too. To achieve this, early testing and gaining feedback from potential end-users of t-government services is needed to uncover yet unknown barriers that may surmount existing categories such as organizational and managerial or technical. This is done in exploratory research that will navigate

through the problem domain, discover unknown phenomena and suggest hypotheses or propositions. Therefore, this essay closes the gap of having a lack of understanding in the context of t-government what potential end users think of tools following the user-managed access paradigm. T-government practitioners and policy makers can use the newly identified challenges to address them in the service design of solutions, that are needed to realize the vision of t-government, e.g. an AEDS.

5.2 Related Work

We suggest that an AEDS might serve as an infrastructure for t-government which will be briefly described first. Thereafter, existing barriers that have been identified in the literature to achieve t-government will be presented. Finally, we argue for the need of doing exploratory research to uncover unknow potential benefits, challenges and barriers.

5.2.1 AEDS as an Infrastructure for T-Government

With an AEDS (see chapter 1.6.4), individuals benefit from a reduction in information fragmentation (Tungare 2009), something that happens, for example, when electronic bills are distributed over several provider-specific online portals. Now, customers are equipped with a tool for exerting informational self-determination in the sense of "vendor relationship management" (Project VRM 2012) which is an inverse of the provider-centric idea of customer relationship management (CRM). An AEDS as an intermediary (a) reduces transaction costs and increases the entire transaction value for all participants (King et al. 2010) and (b) overcomes the problems of information silos (Bannister 2001). Using an AEDS, service provider-specific information silos are replaced by a collaboration of autonomous organizations forming a value chain network (Veenstra et al. 2011) glued together by the individual's decision for sharing. This also supports t-government's aims of citizen empowerment: With an AEDS, individuals have the power to decide with whom they will share information items while, at the same time, they still will have an overview which organizations stores what about them. Moreover, this

will also contribute to realize the t-government's aims to benefit from fully (horizontally and vertically) integrated government services enabling that citizens do only have got or need one contact point for interacting with the public or private sector. To achieve this, all the stakeholders are required to undergo considerable changes – something that needs to be sparked by the introduction of citizen-centric services (Weerakkody et al. 2011). Following this line of argumentation, an AEDS will serve as a tool to surmount "the wall" placed in between a government-centric CRM view and the vision of a citizen-centric, co-production oriented, empowered and engaged citizen (cf. King and Cotterill 2007).

Related work that employs the user-managed access paradigm can be found in the domain of electronic health (Duennebeil et al. 2010). Therein, collaborations of different stakeholders (patients, health care providers, insurance companies) are needed but information silos prevail. To overcome this situation, personal health records (PHR) have been suggested. They contain the lifelong medical information of a patient and are maintained and shared by the patients themselves – in analogy to an AEDS. These PHRs can be stored with private sector based intermediaries such as Google Health or Microsoft HealthVault, also supporting the user-managed access paradigm. Research in the e-health domain (Weitzman et al. 2009) has shown that the acceptance of such PHR systems suffers from issues related to privacy, autonomy, and accessibility.

5.2.2 Barriers to T-Government

Veenstra et al. (2011) developed a literature-based categorization of impediments to achieve the stage of t-government and added empirically derived impediments on the basis of three case studies which involved interviewing three key people from line management and ICT staff. In total, they identified 23 impediments which were grouped into three main categories: governance (7 impediments), organizational and managerial (9 impediments), and technical (7 impediments). Veenstra et al. could confirm twelve literature-based impediments and identify eleven new ones. On the governance level, the main barriers were identified as a lack of a government-wide strategy and vision enabling collaboration in

forms of networks and value chains. On the organizational and managerial level, huge and joint efforts of stakeholders embedded in complex relationships are needed which creates many barriers. In addition, on the technological level, the lack of knowledge to achieve innovations, for instance due to an organization's dependency upon legacy systems, has been diagnosed. Moreover, Weerakkody et al. (2008) identified challenges and issues for achieving t-government. They carried out a case study to empirically identify challenges. Therefore, they interviewed e-government practitioners on their experiences but no citizens. 48 change barriers have been identified which were grouped into four categories (in brackets: number of identified change barriers): organizational challenges (19), process change challenges (11), IS/IT integration challenges (8), and cultural and social challenges (10; such as fear of information technology or organizational resistance).

5.2.3 Exploratory Research to Uncover Potential Benefits, Challenges and Barriers

In order to identify usage potentials and challenges that contribute either to the adoption or non-adoption of technological innovations, researching the mutual relationships between technology as an artifact and users as well as the specific usage context is necessary. This is the basis for developing grounded requirements that can be used for systems and service design. Design Science Research (DSR) (Hevner et al. 2004) is an established approach in Information Systems research in which artefact design, development, and evaluation is often performed in an iterative manner to improve (ideally) a priori defined objectives (Hevner 2007). An AEDS would qualify to follow a DSR paradigm due to its nature of being a nascent concept with no yet fixed implementation. Nevertheless, in the course of carrying out the research activities in this PhD project, the opportunity to follow one or several DSR cycles was not possible. Instead, a related – but, compared to DSR, in a sense reduced – theoretical underpinning of using prototypes as a means for researching innovations was used. Researching new forms of usage with usage experiments, as

suggested by Hanekop (Hanekop 2008), was chosen to identify yet unknow usage patterns, challenges or requirements when test participants interact with a prototype in an experimental setting. Such an experiment helps to gain initial and new knowledge to engage later in more in-depth research to generate more robust design knowledge that is especially needed for the future field of "Service Systems Engineering" in Information Systems research (Böhmann et al. 2014). These "service systems" are complex socio-technical systems that enable value co-creation. As shown in the introductory chapter of this thesis (see chapter 1.6.4) and in the future outlook (chapter 6), an AEDS has the potential to foster value co-creation activities related to the move towards a service-dominant logic (Vargo and Lusch 2004). Therefore, an AEDS as a sociotechnical system is located at the intersection of personal and organizational information management – an emerging research stream in Information Systems research called "Digital Life" (Hess et al. 2014).

5.3 Research Design

As presented in the previous chapters, current research on t-government seems to neglect the individual as a citizen who interacts with t-government services. To overcome this weakness, we will carry out an exploratory user study involving twelve citizens and three representatives of public and private sector organizations (police, insurance and a security company) which will serve as this case study's empirical foundation. In order to enable an in-depth and hands-on experience with the concept of an AEDS, the user study participants worked in a lab-based setting with a prototype executing three business processes (see Figure 6). Finally, a semi-structured interview was carried out and audio-recorded. The interviews were transcribed and qualitative content analysis was performed using the method of a thematic analysis (Braun and Clarke 2006) which has proven to be successful in the field of HCI (Fitzgerald et al. 2008). Following the transcription, initial codes were assigned using the software MAXQDA. After iteratively reading and refining the coding, themes were assigned in a "data-driven" manner. Writing internal project reports

served to review the emerging themes and to discuss them with fellow researcher before defining, naming and compiling them in a final report.

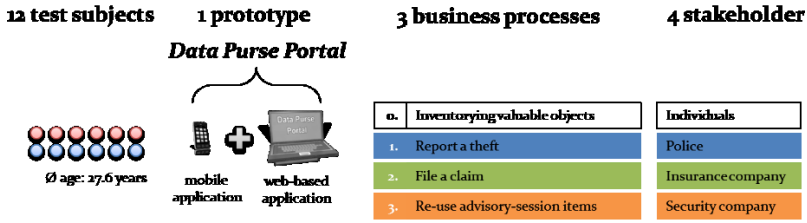

Figure 6: Research design for the evaluation of an AEDS prototype

5.3.1 Measuring User Acceptance

Furthermore, we tried to assess the user acceptance of certain tasks using a set of items as proposed by Liang and Huang (1998). Their work focused on tangible goods that are obtained through e-commerce channels in electronic markets. They aim at identifying acceptance for electronically ordered products using their highly-cited model of constructs. We adapted the wording to fit the intangible tasks that needed to be carried out via the AEDS prototype.

On a 7-point Likert-scale, the participants indicated for each item if they would (a) absolutely not (negative extreme) or (b) absolutely would like to have a task done/service delivered via an AEDS (positive extreme). The rating scale is described in Table 31.

We argue that the labelling of the rating scale's items induces an equidistant scale due to its symmetric construction ranging from the positive maximum ("yes, absolutely"), to a lesser degree described by "very probable" and then followed by "probable" as steps towards the neutral element in the middle of the rating scale. Vice-versa, from the negative maximum ("no, absolutely not"), a gradual improvement towards the neutral element in the middle of the rating scale using the steps "very improbable" and followed by "improbable" is performed. This symmetric construction alludes equal distances between the scale ratings for each item

that are recognizable by the test participants. Therefore, we chose to treat the scale ratings as interval scales and not as ordinal scales which allows us to perform mathematical calculations such averaging the values.

Value	Description of the rating scale
1 (min.)	No, absolutely not.
2	Very improbable.
3	Improbable.
4	Undecided.
5	Probable.
6	Very probable.
7 (max.)	Yes, absolutely.

Table 31: Likert scale to assess user acceptance using the items proposed by Liang and Huang (1998)

The items were related to specific tasks (see Table 32) that had to executed using the AEDS prototype. We asked the participants to rate each main item (number 2. to 10. in Table 32) for each of the three tasks that they had to perform via the AEDS prototype (report a theft to the police, file a claim with an insurance company, get a quote from a craftsman). The items for assessing comparison costs, examination costs, payment cost, site specificity, and physical asset specificity have been omitted for this user test, because they do not fit the setting of the tasks carried out with the AEDS prototype. We did this because Liang and Huang's (1998) model does not imply calculating a score.

Furthermore, a questionnaire focusing on the Technology Acceptance Model (TAM; Chin et al. 2008) was administered in order to measure the test participant's willingness to use the AEDS prototype in the future.

1.	**Perceived acceptance of carrying out transactions with an AEDS**
1.1.	Performing transactions in general with an AEDS
1.2.	Storing personal data in an AEDS
1.3.	Inventorying important documents or objects with an AEDS
2.	**Search cost**
Before carrying out a transaction, you inform yourself about the process. How do you assess the transactions with the AEDS prototype in relation to transactions carried out conventionally?	
3.	**Negotiation cost**
It is usually not allowed to negotiate terms on carrying out business transactions via Web-based services. Compared with the traditional transactions, how troublesome do think is this lack in negotiating support with the AEDS?	
4.	**Delivery cost**
How disturbing do you assess the fact that you do not have to show up in person at an organization to initiate a business transaction?	
5.	**Post-service cost**
How bothered are you, when clarifying questions for an initiated business transaction are dealt within the AEDS prototype instead of using conventional means of communications (e.g., paper-based mail)?	
6.	**Process uncertainty**
Compared to the conventional way, business transactions are carried out (for example, using paper-based mail or seeing a customer representative), how uncertain do you feel about initiating transactions using the AEDS prototype?	
7.	**Product uncertainty**
Compared to the conventional way business transactions are carried out (for example, using paper-based mail or seeing a customer representative), how uncertain do you feel about receiving the wrong product or service by using the AEDS prototype?	
8.	**Human asset specificity**
How important is it for you that a transaction is carried out by a human being?	
9.	**Temporal specificity**
How important is it for you to initiate business transactions anytime?	
10.	**Control costs**
Compared to the conventional execution of business processes, how much effort do you have to check and control the transaction and data submitted using the AEDS prototype?	

Table 32: Items for assessing user acceptance (adapted from Liang and Huang (1998))

5.3.2 Measuring Willingness-to-Pay

To identify potential future usage of an AEDS and identifying potential tasks offering the most benefits to customers or citizens, we performed a detailed task-based analysis using the willingness-to-pay as an indicator. Therefore, we asked the test subjects how much they are willing to pay for tasks and services which can be offered or executed via an AEDS. The willingness-to-pay serves as an indicator for how important a specific task is to our test participants. The test subjects received an itemized list of tasks (see Table 33). For each of the tasks, the test subjects gave their opinion on a 5-point Likert-scale with the extreme poles indicating (a) how much they want to do the task themselves (positive maximum) or (b) have the tasks done for them (negative minimum). Except for the minimum and maximum, no other items of the rating scale have been labelled. Therefore, the ratings can be interpreted by the participants as equidistant which allows us to calculate, for example, averages. Additionally, the participants should award a fictitious price tag to each specific task (see Table 33).

Several methods for measuring willingness-to-pay (WTP) exist (Breidert et al. 2006). We have chosen to follow the approach of a Vickrey auction. This means that the bidder with the highest bid succeeds but only has to "pay" the price of the second highest bid. As an incentive, a small gift was offered to the test subject that succeeded in successfully bidding most frequently on the second highest "price". Despite the problems associated with a direct survey of WTP, especially for complex and unfamiliar goods (cf. Breidert et al. 2006), we nevertheless followed this approach to get a first impression how the WTP for an AEDS will look like.

1.	**Inventorying possessions**
1.1.	Inventorying possessions as a general activity
1.2.	Have an overview of one's possessions
1.3.	Inventorying receipts
1.4.	Capture detailed data about a purchased object
2.	**Report a theft at the police**
2.1.	Reporting a theft as a general activity
2.2.	Looking for and collecting documents related to reporting a theft
2.3.	Completing forms and giving details related to reporting a theft
2.4.	React to clarifying questions after having reported a theft
3.	**File a claim with an insurance company**
3.1.	Filing a claim as a general activity
3.2.	Looking for and collecting documents related to filing a claim
3.3.	Completing forms and giving details related to filing a claim
3.4.	React to clarifying questions after having filed a claim
4.	**Getting a quote from a craftsman**
4.1.	Getting a quote as a general activity
4.2.	Looking for and collecting documents related to getting a quote
4.3.	Actually carrying out the task of getting a quote
5.	**Carrying out business transactions with public administrations/organizations in general**
6.	**Administrate my personal "official" life with public authorities or private organizations.**
7.	**Being reminded for tasks**
8.	**Being reminded for appointments and deadlines**
9.	**Control and know who has stored data about me.**

Table 33: Items for estimating the willingness-to-pay

5.3.3 Description of the Prototype

The prototype is based on a Web application (Reber 2013) (see Figure 7) and a mobile application developed on the Android platform (Peduzzi 2013) (see Figure 8) which both have been developed applying a user-centered approach following scenario-based design (Rosson and Carroll 2002).

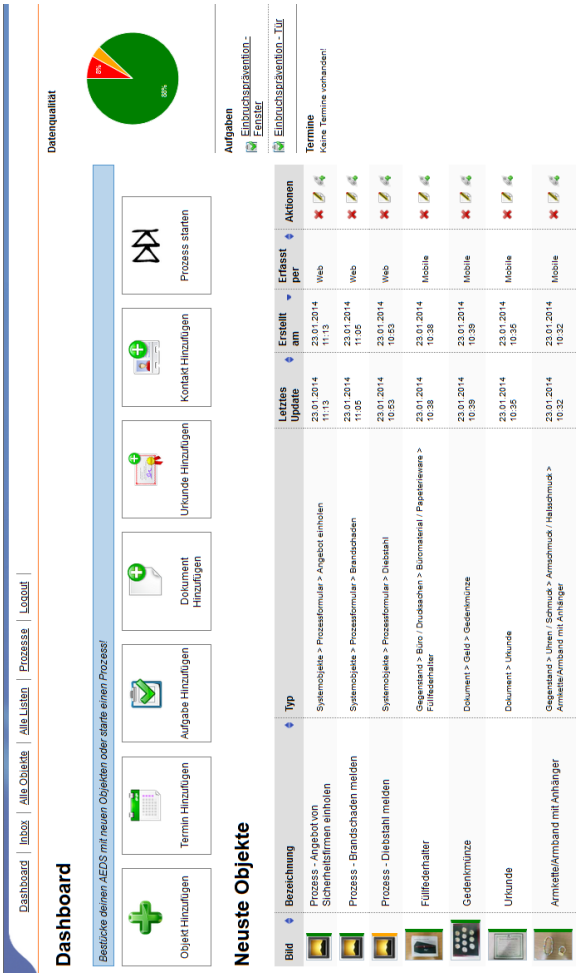

Figure 7: Screenshot of the Web application (Reber 2013)

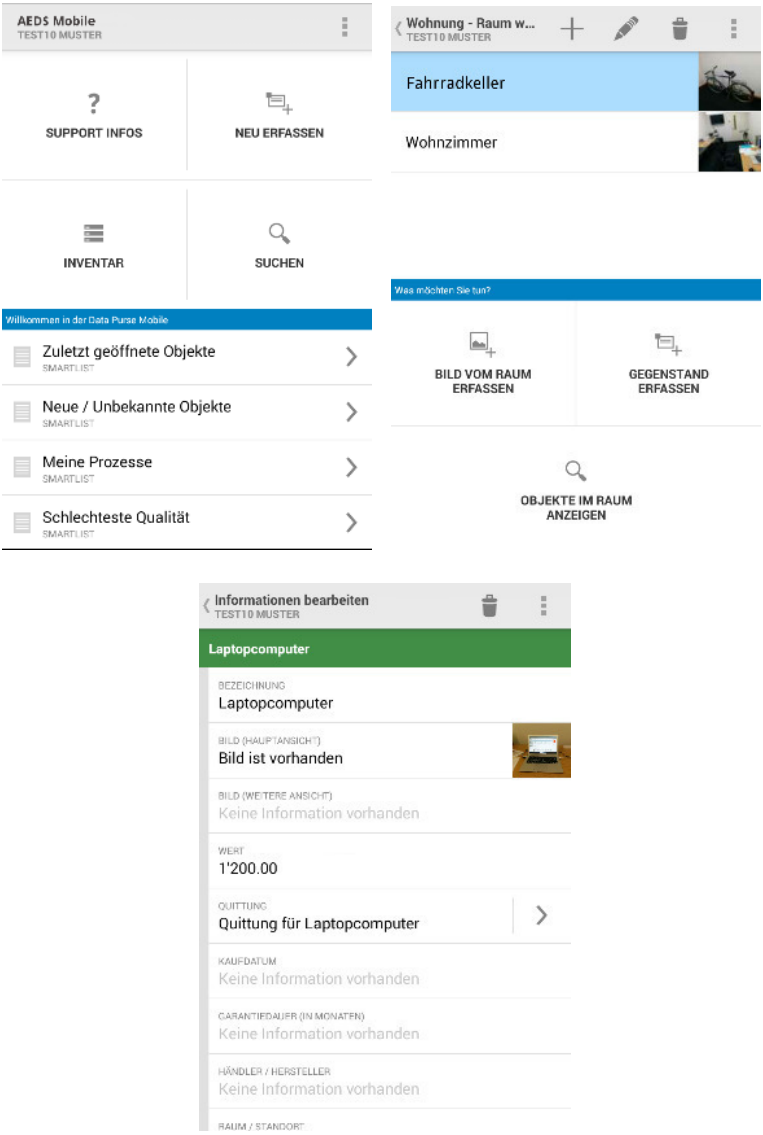

Figure 8: Screenshots of the mobile application (Peduzzi 2013)

With the help of the AEDS, the test users inventoried physical personal items including documents or certificates. Each item had to be assigned a category which has been originally taken from the police's software used to describe stolen or lost belongings but has been modified for the purposes of this experiment. Depending upon an object's category, the mandatory and optional fields change. Objects can be linked, aiming at grouping related things, for instance, the photograph of a bike and its bill. The AEDS offered process support through its Web application. After starting a process (i.e. choosing the "life-app" such as "file a claim with your insurance company"), a web form was presented to the test participants requesting them, for example, to describe what happened. The objects, which have been inventoried before, could be grouped into lists and be attached to a process. Furthermore, the prototype of the AEDS included an inbox in which all elements received via an individual e-mail address were unified, such as to-dos, photos or materials received during an advisory session. Additionally, a messaging component has been implemented in order to allow communication of an individual with an organization related to a certain process.

5.3.4 Details on the Experimental Setup

In a laboratory study, twelve participants (six females, six males, average age = 27.6 years, see Table 34 for details) tested the prototype of an AEDS. They have been recruited using a public server where test participants could voluntarily register for experiments. Their self-described computer-knowledge ranged from professional (7), to advanced (3) and lay persons (2); everyone used the Internet daily. At the beginning, the test subjects were briefed how the test will be carried out and that no individual assessment is performed because we are rather interested in the participants' overall impressions. The participants had to work upon three tasks that were designed to realistically mirror exceptional, but nevertheless, common business transactions with a sufficient degree of complexity: (a) to report a theft to the Police, (b) to file a claim with an insurance company and (c) to get a quote from a security company based on some fictitious vulnerabilities of the home such as a weak door.

ID	age	gender	profession
P01	21	w	accountant
P02	60	m	IT-consultant
P03	23	w	event manager
P04	22	w	student
P05	31	m	researcher internet technologies
P06	21	m	student
P07	23	w	student
P08	27	m	flight attendant
P09	23	m	student
P10	32	w	accountant / student
P11	25	w	research assistant
P12	24	m	student

Table 34: Detailed description of the test subjects

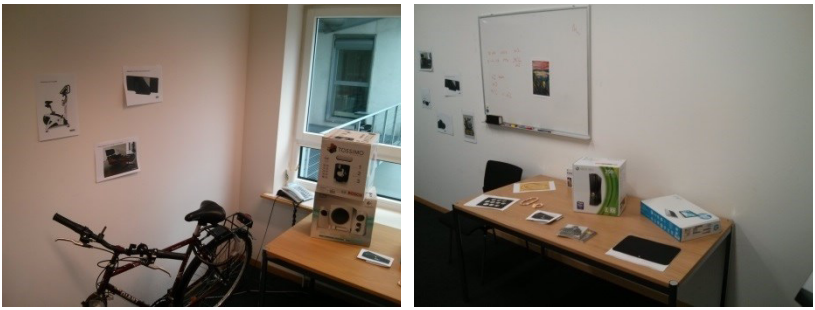

Figure 9: Room for the user test

First, all the test subjects received a short crime prevention counseling session by a trained member of our research group. Thereby, some fictitious vulnerability like a weak door or badly secured windows has been documented electronically and with a photo; they were transferred into test subject's individual inbox as to-dos. After that, the test supervisor provided the clients with a short introduction how to use the tools before they embarked on their own following a detailed protocol. The first part consisted in inventorying objects and documents which were placed inside the laboratory (a bike, photos of valuables, bills, etc. see Figure 9).

The second part of the experiment consisted in carrying out fictitious business transactions using the AEDS. The test subjects had to (a) report a theft to the police, (b) file a claim due to a fire in their home to the insurance company and (c) get a quote from a security company in order to fix the security issues that had been detected during the initial crime prevention advice session. While carrying out these tasks, the test participants also used the messaging function and interacted with real representative from the police or insurance company, for instance, to clarify questions. A semi-structured interview closed the two hour-session.

In the end-to-end test of the prototype of an AEDS, representatives of the police and an insurance company were involved, too. They interacted with the study participants through the AEDS prototype by answering or asking questions through a messaging component. Furthermore, they evaluate the usefulness of the exchanged information items that have been captured by the study participants (taking photos of valuables and electronically attaching receipts to build an inventory list). As the third representative from an organization, the security company gave their feedback in one single session because the fictitious vulnerability was always the same for all of the test subjects.

5.4 Results

First, we will report on the findings in relation to the user's acceptance and willingness to use and pay for services via an AEDS. Then, the findings from the semi-structured interviews based on the thematic analysis (Braun and Clarke 2006) are presented, starting with the customer/individual perspective, and finishing with the service provider perspective.

5.4.1 Willingness to Use an AEDS and to Pay for It

During the qualitative interviews, the test subjects were asked if they could imagine using an AEDS in the future. Nine subjects answered with yes. One could not imagine using such a service, another participant was unsure about the process-support capabilities. Another participant asked what would be the benefit compared to already existing technologies.

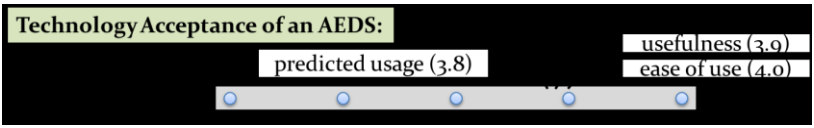

Figure 10: Technology Acceptance of an AEDS

The overwhelming "yes" towards a future use of an AEDS must be put into contrast with the less euphoric but still positive findings from the TAM questionnaire (see Figure 10): All participants judged on a 5-point Likert scale (1 = negative; 5 = positive) the dimension "ease of use" with 4.0, "usefulness" with 3.9 and "predicted usage" with 3.8. Taking into account the TAM and the qualitative ratings, our test participants could imagine a future use of AEDS and they are able to recognize a positive utility.

Moreover, we inquired about the test subject's WTP (Table 35 and Table 36) for services and tasks supported by an AEDS. Besides asking for their WTP, we also asked about a task's *attractiveness* rated on a 5-point Likert scale if they wanted to perform the described task themselves (value 1) or have it done for them (value 5). Because of the symmetric nature of the scale items, we assume equidistance which allows us to calculate the average in order to compare the different tasks based on the arithmetic means of all test participant's ratings of a task's attractiveness.

As you can see, the WTP in CHF ranges from fairly low amounts for simple tasks (being reminded about tasks) to higher amounts for more complex tasks like administrating one's life or controlling the use of one's personal data. WTP seems not to correlate with the attractiveness of the tasks, i.e. that something you will pay a higher price for should be necessarily done by someone else on behalf of you. As an example, inventorying personal belongings is regarded as a task that people would pay for but, at the same time, they want to do it on their own.

task	bid in CHF	attract-iveness
Being reminded about tasks.	9.10	3.18
Answer requests from an insurance company.	9.70	2.73
Write to a craftsman to get a quote.	10.20	2.91
Answer request from the police.	11.27	2.60
Get a quote from a craftsman.	13.20	2.82
Seize data digitally about a physical item.	15.27	3.46
Collect documents for getting a quote from a craftsman.	15.40	3.27
Being reminded about deadlines and appointments.	15.41	3.55
Complete forms and provide data for the police.	19.27	3.60
Report an item as stolen towards the police.	20.73	2.81
Collect documents for reporting an item as stolen with the police.	22.63	3.90
File a claim with an insurance company.	22.70	3.27
Collect documents for filing a claim with an insurance company.	25.40	4.18
Complete forms and provide data for an insurance company.	29.20	3.73
Have an overview of my belongings.	32.18	2.00
Doing business with public administration authorities/organizations.	32.20	3.46
Control/understand where personal data is used by whom	42.30	2.27
Inventorying personal belongings	44.46	2.81
Capturing receipts or bills digitally	46.55	4.18
Administrate my life with respect to public authorities or due to private contracts.	58.60	3.18

Table 35: Willingness-To-Pay per task (sorted ascendingly by bid)

The WTP for the task "collecting a document" is treated differently depending upon the context: In the context for the police and an insurance company, the WTP is higher than collecting documents for a craftsman. This opens up the interpretation that tasks which will receive a tangible benefit are valued higher (for example, collect documents to file a claim and get reimbursed) than less specific tasks.

#	task	bid in CHF	attract-iveness
1	Have an overview of my belongings.	32.18	2.00
2	Control/understand where personal data is used by whom	42.30	2.27
3	Answer request from the police.	11.27	2.60
4	Answer requests from an insurance company.	9.70	2.73
5	Report an item as stolen towards the police.	20.73	2.81
6	Inventorying personal belongings	44.46	2.81
7	Get a quote from a craftsman.	13.20	2.82
8	Write to a craftsman to get a quote.	10.20	2.91
9	Being reminded about tasks.	9.10	3.18
10	Administrate my life with respect to public authorities or due to private contracts.	58.60	3.18
11	Collect documents for getting a quote from a craftsman.	15.40	3.27
12	File a claim with an insurance company.	22.70	3.27
13	Seize data digitally about a physical item.	15.27	3.46
14	Doing business with public administration authori-ties/organizations.	32.20	3.46
15	Being reminded about deadlines and appointments.	15.41	3.55
16	Complete forms and provide data for the police.	19.27	3.60
17	Complete forms and provide data for an insurance com-pany.	29.20	3.73
18	Collect documents for reporting an item as stolen with the police.	22.63	3.90
19	Collect documents for filing a claim with an insurance company.	25.40	4.18
20	Capturing receipts or bills digitally	46.55	4.18

Table 36: Willingness to carry out tasks oneself (1 = do on my own; 5 = have it done for me by someone else)

By comparing the attractiveness and the price for a bid visually (Figure 11, numbers are referring to task id in Table 36), we can identify at least two clusters (see also Table 37 and Table 38): Cluster 1 consisting of tasks 1, 2, 6, 10. Task 20 can either be united with the aforementioned cluster 1 or regarded as a separate cluster 2. The rest of the tasks is in cluster 3.

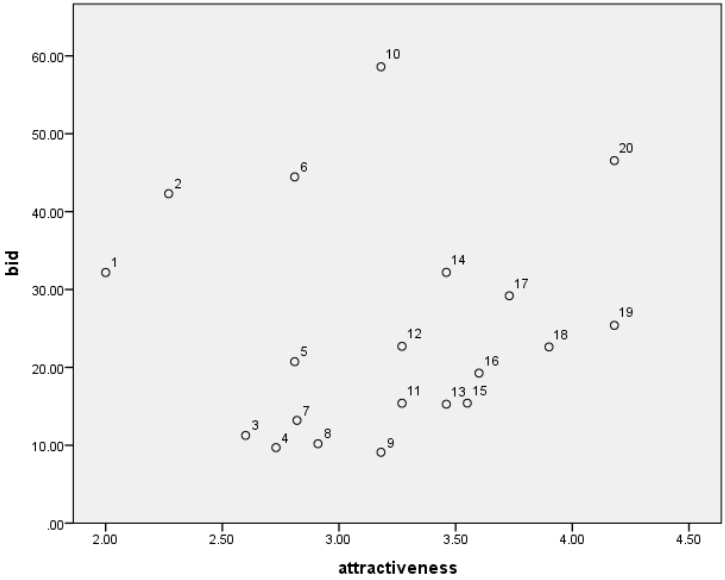

Figure 11: Comparing a task's value (as a bid) and attractiveness (1 = doing it oneself; 5 = having it done by someone else)

#	cluster	task	bid in CHF	attract-iveness
1	1	Have an overview of my belongings	32.18	2.00
2	1	Control/understand where personal data is used by whom	42.30	2.27
6	1	Inventorying personal belongings	44.46	2.81
10	1	Administrate my life with respect to public authorities or due to private contracts.	58.60	3.18
20	2	Capturing receipts or bills digitally	46.55	4.18

Table 37: Tasks in cluster 1 and 2

#	cluster	task	bid in CHF	attractiveness
3	3	Answer request from the police.	11.27	2.60
4	3	Answer requests from an insurance company.	9.70	2.73
5	3	Report an item as stolen towards the police.	20.73	2.81
7	3	Get a quote from a craftsman.	13.20	2.82
8	3	Write to a craftsman to get a quote.	10.20	2.91
9	3	Being reminded about tasks.	9.10	3.18
11	3	Collect documents for getting a quote from a craftsman.	15.40	3.27
12	3	File a claim with an insurance company.	22.70	3.27
13	3	Seize data digitally about a physical item.	15.27	3.46
14	3	Doing business with public administration authorities/organizations.	32.20	3.46
15	3	Being reminded about deadlines and appointments.	15.41	3.55
16	3	Complete forms and provide data for the police.	19.27	3.60
17	3	Complete forms and provide data for an insurance company.	29.20	3.73
18	3	Collect documents for reporting an item as stolen with the police.	22.63	3.90
19	3	Collect documents for filing a claim with an insurance company.	25.40	4.18

Table 38: Tasks in cluster 3

It seems that in cluster 1, all tasks are grouped that are highly valued by the test subjects and that the participants want to carry out these tasks by themselves. The separate cluster 2 contains a task which is highly valued, but the test subjects think that it should be performed by someone else for them. The rest of the tasks form the biggest cluster 3 which have received a rather low to medium-high valuation and should be performed neutrally or on behalf of the test subjects by someone else.

There is a positive correlation between the height of the bid and the desire to have the task done on behalf of oneself of the tasks in cluster 3: The higher the value is for the customers, the more they want to have the task done for them by someone else. This is positively correlated and highly significant (double-sided t-test with $p=0.009$, $n = 15$ tasks in cluster 3). The tasks in cluster 1 and 2 do not follow this pattern. They seem

to have a more controlling and creative character which qualifies them to be preferred for being handled on your own. For example, such tasks are obtaining an overview of your belongings or answering requests. These higher-level tasks involve the conscious argumentation (answer requests) and deciding individually about the correctness of the use of personal information.

5.4.2 Results from the Qualitative Interviews

In the following sections, the findings from the semi-structured interviews are presented. Quotations are added in order to illustrate the identified themes based on the interpreted data, an approach that is common in qualitative analysis (Braun and Clarke 2006). They have been translated into English by the author of this thesis. The IDs used refer to the participants presented in Table 34 on page 191).

5.4.2.1 Customer/Individual Perspective

General positive impressions: The test subjects were asked to tell what they liked about the idea of an AEDS as experienced in the prototype. The ease of use for capturing objects was welcomed positively (P02, P03, P04, P05, P06, P08, P09, P11): "I liked the inventorying part. I think that I would do this myself, too." (P5). Also, the easy execution of transactions was a recurring theme (P08, P09, P11), for example, described by P09: "It is a good thing that you can forward items immediately, for instance to the police or an insurance company." Potential for savings in time (P07) and money or effort ("I liked the simplicity, and also, that I did not need to send requests via postal services.", P06) due to only capturing items once were generally recognized. The idea of bundling photos with receipts or metadata was perceived as something helpful (P01, P02), especially when objects get lost or get broken, for instance, in case of theft (P01, P05, P07; "I like it very much that I have everything at one place just in case something happens", P05). Besides, our participants positively remarked that they have an overview of their belongings (P01, P02, P03, P11).

Mobile vs. stationary usage: In general, the test participants preferred to use the mobile phone for inventorying objects and documents (P03, P04, P06, P09, P11): "Everything was extremely easy, notably capturing objects. I was walking with my mobile phone throughout the place and photographed everything. You cannot make it easier." (P11) The main reason which was given in the subject's explanation is the easy way to take photographs in the mobile app and that they, during the course of tasks, have already been working with the mobile app before. Two participants (P10, P11) noticed that the immediate synchronization was a nice feature which supported them in their style of working: first take photographs with the mobile app and then check or add metadata with the laptop because "I prefer writing on a computer because typing longer texts on the mobile phone feels unpleasant." (P10)

Concerns about the efforts to populate an AEDS: Populating an AEDS with enough data initially was regularly identified as an obstacle (P01, P04, P11, P12): "Of course you have to type in everything. The more is in there, the better it will be. But you only do this once. Normally, you do not buy everything at once." (P01). Keeping things up to date was identified as an issue, too: "I do not know how realistic it is that I will type in all my objects that I will buy. I am sceptic about it. I know myself and that I am not so disciplined." (P02).

Concerns about storage security and unauthorized access: Many test participants said that they did not ask themselves where the data will be stored during the experiments (P04, P05, P06, P08, P10, P11) – only the question by the interviewer triggered this thought. Of these participants, one explained that "I would have asked myself if I encountered this service somewhere on the Internet. Then, I would have asked myself how trustworthy this service is." (P06) One test subject expressed directly its concerns about the location where the data was stored (P08), and two other participants hoped that no cloud storage is involved and data is stored only locally (P05, P12) – despite the obvious synchronization between the mobile phone and the laptop. Others participants (P03, P07) expressed a diffuse feeling of threat:

"I am troubled that so many data is stored somewhere. That causes a feeling of insecurity. I had this thought while working with the laptop. Someone will be able to get access to these data. Not that anybody will be interested in knowing that I own a personal computer at home, but you never know." (P07)

The fear of someone else hacking into a personal account was expressed by half of the participants (P01, P02, P03, P07, P10, P11). The spectrum ranged from a fatalistic "Someone will always be able to gain access." (P07) to a dedicated tradeoff between risk and benefits ("The personal benefit of having access from everywhere is higher than potential risks that these data could actually be of use for someone else.", P09). The impression of the test subjects was that they still wanted to be into control about their data (P02), especially the country where their data is stored ("It would be ideal if the software product is located in Germany, Switzerland or the European Union.", P08). One participant (P12) mentioned that he changed his behavior a lot after the disclosures related to the National Security Agency of the United States of America in 2013. Explicitly, this person demanded an end-to-end encryption of the exchanged messages before he would engage in business transactions using an AEDS.

Which organization should run an AEDS? One test participant (P06) expressed his favor towards having an AEDS run by a well-known organization running a trustworthy looking Web site. Three test subjects (P05, P06, P11) mentioned that they would not want a start-up company run an AEDS; they would rather prefer an insurance company or, at best, the public administration offering such a service:

"I would feel fine if the service would be run by the public authorities or, I would not even mind, by an insurance company. This would be far more sympathetic for me than an independent but unknown company. If I do not know the name, I can hardly estimate who is behind a company and what is the company's culture." (P11)

What people like to store in an AEDS: Two test subjects (P10, P11) mentioned that their personal belongings were of too little value in their current state of life and therefore they would not need the inventorying functionality ("I do not own so many valuables.", P11). Generally, only the most expensive objects (cars, electronics, and furniture) seem to be worth the effort of capturing data and metadata (P01, P05, P06, P08, P12). "Yes, the more expensive objects starting from 200-300 CHF. Below that threshold, I would do it less probably because the effort-benefit ratio does not fit." (P12). Furthermore, unique documents like attestations or certificates were regarded as qualified for storage in an AEDS (P03, P04, P05, P10), for example, as mentioned by P10: "I asked myself if documents or certificates should be stored there, too. I think yes, because one could benefit from the overview." Moreover, two participants (P06, P09) explicitly referred to memorabilia or objects bearing a sentimental value that should be saved in an AEDS, too: "I would like to store objects that have a certain monetary or emotional value. Ultimately, I do not know if these objects would be of interest to an insurance company or the police – but they are nevertheless valuable to me." (P06). One participant (P05) suggested that he would like to store meta-lists with documents instead of the documents or representations of the documents themselves in order to reconstruct what one had owned. He thought that this might be more helpful because "If my birth certificate is burnt, I will have to get a new one anyway. I would have a photo of it, but it will not help." (P05).

What people do not want to store in an AEDS: The spectrum of information items not to be stored in an AEDS is quite divers as is the spectrum of things that should be stored in there (see also chapter 3.4.1 on page 108 in essay 2 for an analysis of real EDS user's stored information items). Special notice has to be paid to financial data: Two participants (P03, P05) spontaneously named financial data (bank statements as well as pay slips) as being inappropriate to be stored in an AEDS. Credit card data was also disregarded to be an item that should be stored in an AEDS (P01). These findings seem to be in contrast with the findings of real EDS users. As an explanation, the AEDS prototype users were "virtually" mus-

ing about potential documents whereas the current EDS users did actually store information items in an EDS. And, one of the EDS service providers whose customers have been interviewed, worked in close cooperation with a bank that delivered its monthly statements directly into the EDS of a user. Thereby, some users might have been either surprised or have been positively convinced about the EDS service's suitability to accommodate for such "sensitive" information items. Personal information as information items not to be stored in an AEDS were mentioned twice (P01, P10) alongside with photos in general (P01), and certificates and documents: "I cannot make friends with the idea of storing documents like school certificates in an AEDS. That does not make sense for me. As long as nobody convinces me, I would not do that." (P06). On the other extreme, two participants (P05, P09) favored the all or nothing approach: "If you have committed yourself to such a solution, using it only with parts of my documents and data does not make sense." (P05) or even expressed a view such as "I do not have sensitive data." (P04). What items should be stored is, according to three participants (P02, P03, P12), dependent on the security measures or the country where the service is located. These views do also underpin the idea that an individual structures its information items in different value zones (see chapter 3.5.2 on page 127). Which information items do belong in which zone is a highly-individualized decision – as it is expressed in by the AEDS test subject's opinion that was not primed or influenced by an EDS services actual usage.

Combining advisory sessions with processes in an AEDS: The test subjects thought that transferring information items gathered during an advisory session like the crime-prevention advisory at the beginning of the user study was something positive (P03, P04, P07, P10, P11, P12). Reusing data was considered an advantage and one participant even expressed his favor for getting rid of paper at all:

> *"I thought it was very handy, and I was surprised that it was that fast with the photo. I liked the minutes of the advisory session." (P03)*

> *"I think the idea is handy. If results from other advisory sessions can be transferred and forwarded, too, then it makes sense." (P04)*

"I think it is useful. The question is, for example, when I would receive something printed from a banking advisor why I should receive it again electronically. If I receive it only electronically, then it is useful." (P07)

"If it is usable for any advisory session, then it is a good invention. From my perspective, we could abolish paper at all." (P09)

"I think this makes sense. The more information is in an AEDS, the more helpful it will become." (P12)

Preferences for structures and structured processes: Being provided with structures for the description of objects and have a structure to forward items systematically in business processes was judged (P02, P03) as a benefit ("I think it is good to have structures. They help me to know what an insurance company would like to have things described", P03). With respect to the crime prevention advisory session at the beginning, one participant (P11) noted that there might be a danger of just letting something through on the nod which was associated with too much structure hindering own, critical thinking:

"It looks like someone would say what I should do next, and then, I have to do that. I would not need to make own thoughts what I want. But I feel that I would lack a more intense involvement. It is a bit like being left outside: A specialist arrives and tells me what to do. And I would do that although I did not make my own thoughts about it, for instance, if I really need a window grille. You are tempted to just click. I especially would prefer the direct contact with a craftsman to have him seen before. With an insurance company where bureaucratic processes rule, I would be more inclined to let these run and be guided through by a program – in contrast to things I like to have an influence on." (P11)

Problems of describing and categorizing objects: Although a classification scheme was suggested, four test participants (P06, P07, P08, P09) expressed that they missed the opportunity to define new categories themselves. Some other participants mentioned that they did not know which data they should provide because there are so many options, or, that they were lacking essential information. Eight participants said that

they would have worked more carefully and would have seized data in more detail if they had performed the inventorying at their own home (P05, P06, P08-12).

Uncertainties about objects sent as attachments: The messaging component of the AEDS prototype was considered by the test subjects as the place where answers to requests on objects should be placed (P05-12). Only three test subjects (P05, P11, P12) thought about modifying an object's metadata directly instead of typing it in the messaging component. The main reason for not doing this was that they were not sure whether this update will be transferred and signaled to the organizations the object was sent to as a process-attachment. Some participants (P08, P09, P11, P12) mentioned that they were not sure if attaching an object also includes the linked objects, such as the invoice of a bike and were unhappy about this lack of transparency which information items are actually transmitted.

5.4.2.2 Organizational/Service Provider Perspective

In this chapter, the findings with respect to the organizational/service provider's perspective are grouped according to the themes identified in the transcribed interview data.

General impressions: The police representative focused his answers on the current prototype and seldom generalized to the overarching concept of an AEDS. He considered the current prototype inappropriate and less helpful than the current practices ("The data I received was so rudimentary that I could not use it for compiling the official files.", police representative). Nevertheless, if the right information items would have been provided by the customers and a deep integration into the police's inter-

nal IT systems had been performed, then he might see utility for the concept of an AEDS – something he experienced with already available police services online, such as reporting a stolen bike using Suisse ePolice[26].

On the contrary, the insurance company's representative was already quite convinced by the data received through the prototype of an AEDS and thinks that such a concept bears great potential in the future: "From an insurance company's perspective, this is a good approach. I liked the current system. That is an excellent rating you can get from an insurance company." (insurance company representative) He also thinks that customers' willingness to use such a service has increased – something which has been unthinkable ten years before.

The security company's representatives think that receiving pictures is insufficient to come up with a conclusive offer. The level of details might be sufficient to get an impression that a door may be too weak or that the windows are not properly secured, but the whole context of the house or flat is lacking which have to be considered to suggest a comprehensive solution. If a huge number of pictures had been taken that could reflect the entire context of a house, elaborating an offer was regarded as feasible – but the effort and expertise needed for taking these pictures is huge and thus, an on-site visit is more appropriate.

Key benefits: According to the insurance company's representative, two things are decisive: the data submitted with the claim (is it helpful for processing claims?) and the supporting documents such as invoices. The current prototype of an AEDS supports both business process requirements in a helpful manner: "If we can communicate efficiently with a customer, it is worth thinking to go further in this direction. You probably will not be able to save half of the time needed to finish the business process but if a critical mass of users would be available, it nevertheless will

[26] https://suisse-epolice.ch/epolice/ - A virtual police station to report, for example, bikes as stolen or vandalism.

be an alleviation for our organization." (insurance company representative) This quote also shows the key challenge: the need for a critical mass of customers. Only if a sufficiently large volume of customers exist, effects of economies of scale will arise. Before, the costs induced by this new way of working will not be justifiable and too little benefits for the organization would arise. Especially in the context of bulk processing large numbers of claims, such as the loss or theft of bikes or mobile phones, a high number of correctly completed forms that are filed with a claim and where an invoice or bill as a certificate of possession and value is attached simultaneously, could speed up the processing cycle times for all cases. Phone calls to inform the customer about the status of his case and/or requesting invoices or other certificates to document the value of his possessions, could be reduced. "Each open case costs money. A client calls the call-center and a case will be opened and further steps are explained to the customer. Then, we have to wait about a week for the requested supporting documents before being able to close the case. An AEDS would bring along the opportunity to close a case earlier." (insurance company representative)

The police representative was more in favor of the current way how the business transactions are carried out. His main point of concern was with the data quality he judged as insufficient due to the lack of data uniquely identifying an object, such as a serial number. If the data quality had been better and the data could have been transferred by one click directly into the police's IT backend-systems, then he could think of AEDS as bringing improvements to the current situation. At the current stage, the advantage plays only on the client's but less on the police's side was his opinion. Nevertheless, he recognizes the AEDS's potential for image and efficiency improvements: "The software is modern and contemporary. It is something normal for the younger people. The police want also to keep pace with modern technology. With an AEDS, widespread criminal offences can be dealt with a smaller team." (police representative)

The security company did not see any particular benefits of receiving photographs depicting and describing a house's vulnerability. The representatives said that they acknowledge that the customer had received the crime prevention advisory before and they see what had been suggested. But nevertheless, they want to use their own expertise to come up with a comprehensive and tailored offer which is based on an on-site visit of the customer.

Quality of data: The insurance company's representative was satisfied with the quality of the data and the photos of the objects and documents they received. For each item, the date of purchase and value at that time was regarded as the most important data item. A unique identification of an object, for instance by its serial number, is unimportant to the insurance company (at least for objects originating from mass production). On the contrary, the police representative was totally dissatisfied with the data that was seized by the test customers. According to him, the important parts identifying an object uniquely such as serial numbers or special attributes (like a Mickey Mouse-shaped bike bell attached to a bike) have been omitted. The underlying rationale is, what happens if an item reported as lost or stolen is found and how it can be attributed with certainty to its owner. Therefore, the date of purchase and the object's value are of no importance to the police but only the unique identifiers:

> *"Serial numbers, frame numbers, and engravings are the most important attributes to identify objects such as bikes or jewelry. Just naming the brand is useless if it is an object originating from mass production and we have to prove that it belongs to a certain person. During the test, just naming the brand and color was too unspecific. But since we have to document all the attributes someone provides, we nevertheless have to note them down." (police representative)*

The police representative and the insurance company representative also assumed that – with respect to already available online services – data quality is better when the people want something from the police or an insurance company. Only then, people pay more attention to provide complete and sound information. The organizations offer their services

but do not see their primary duty in urging the client to provide comprehensive and correct data. "Someone reporting a loss or theft to the police demands something of us [the police]. Some customers had the feeling that it is the police that is responsible for collecting correct serial numbers with each bike store. But it is the customer who has to provide correct and complete data." (police representative) "If we need the invoice, for example, of a mobile phone, we actively remind a customer two more times. If he does not answer, we will not pursue the process further." (insurance company representative) The security company's representatives argued that just having a look at the pictures submitted via an AEDS is insufficient to find out about the context of a house. "Pictures would not be so helpful. We only can start after having seen the object ourselves. It is more trustworthy and more specific for the customer when we do an on-site visit instead of just sending him an offer. [...] Otherwise, it is like ordering a vacuum cleaner from a catalogue: There, I have seen the picture and then it would work fine. But an on-site advisory session is more professional because you can respond to a customer's needs more individually." (security company representative)

Role and quality of photos: According to the police representative, the photos submitted during the user test were of insufficient quality to be used for extracting data necessary for their official search, except for jewelry. The test participants have not been given detailed instructions on how to take photos – they acted naturally. The police representative stated that pictures ideally are taken from multiple perspectives (front, side) and show clearly identifiably properties of an object (such as the imprint of a coin). Just photographing a television or a computer showing the manufacturer and type is insufficient due to the lack of uniquely identifiable characteristics, such as a serial number or a sticker attached to a laptop. For jewelry, the police representative noted, that pictures can indeed help to give clues how to describe them better (for instance, if it is a plain coil chain or curb chain). Moreover, he suggested that placing a scale besides an object would help to estimate its size better, for instance the length and width of jewelry which are necessary data to be seized for filing the official search. The security company's representatives thought

that pictures are just able to give a first impression but do not contribute to a holistic understanding which is necessary for the elaboration of a tailored offer. They even thought about potentially deterring customers by telling them via e-mail that they would need to mechanically secure, for instance, their entrance door. If this had been suggested, so the representatives' argumentation, during an on-site visit, such a measure could be put into context and therefore the customers would accept them more readily.

Dealing with (anticipated) needs for clarification: Nowadays, the police representative remarked that e-mail was the preferred way of obtaining information or additional data which could not be provided during a personal appointment in order to describe the loss or theft of an object. This asynchronous medium offers the possibility that the client can answer the message whenever he or she wants, especially after having looked up the missing information, for example, a serial number, at home. If the person had been called in their office, this had been fruitless. Besides, the police offices work in shifts and therefore responding to e-mails is also more convenient for them. On the contrary, the insurance company currently focuses on establishing a personal contact with a client over the telephone. Their rationale is to avoid any misunderstandings by immediate clarification in a personal talk which will save time and frustration on both, the client and the insurance company's side. Referring to the messaging component of the AEDS prototype, the aforementioned views of the police and the insurance company persisted. The insurance company's representative was unsure if an electronic processing with an AEDS might create ambiguities leading to a spiral of questions and answers. But the police representative thought that such a component is sufficient to communicate about the details which are lacking and explicitly demanded by the police. The feasibility of providing a live chat in real time with the responsible person in the organization was dismissed as impossible by the police and the insurance company due to practical reasons. This also reflects the test customer's perception that they would not expect a real-time answer.

Status updates: The insurance company's representative stated that a customer should always be informed what is going on at the moment. On the contrary, the police's representative answered that a customer does not receive status updates because this would cause too much efforts. If an object is found and the owner could be identified using a serial number, for example, then, the owner will be contacted first via telephone. Only if the case has been submitted electronically via Suisse ePolice, the customers receives an e-mail after which they go to the police station.

5.5 Barriers to T-Government in the Context of an AEDS

Based on the empirical data elaborated in the user study and applying the thematic analysis as a method, four barriers to achieve the stage of t-government using an AEDS are identified (they are summarized in Table 39).

We acknowledge that other factors originating from other components that contribute to t-government might lead to further barriers. However, we argue that due to our research design the identified barriers are related predominately to the AEDS.

#	barrier
1	Offering unfamiliar services that have a character of experience-goods will be a barrier to an AEDS' adoption.
2	Not fulfilling common service expectations of the customers will result in a barrier to an AEDS's adoption.
3	Failing to establish contextual integrity will cause a barrier to the adoption of an AEDS.
4	Failing to establish and run an AEDS as a multi-sided platform with an attractive business model will be a barrier for the adoption amongst all stakeholders.

Table 39: Barriers to t-government with respect to AEDS

5.5.1 Offering Unfamiliar Services Perceived as Experience-Goods

The results from the user study show that the study participants preferred clearly structured processes like filing a claim with an insurance company. The study participants were asked to rate which future business transactions they would like to carry out with an AEDS (Likert-scale ranging from 1 = no, never; 4 = undecided; 7 = yes, absolutely), as introduced in chapter 5.3.1.

task	mean
getting a quote from a security company	3.36 = improbable
managing personal data	4.55 = "undecided" (4) and "probably" (5)
report a theft to the police	5 = "probably"
inventorying important objects	5 = "probably"
file a claim with an insurance company	5.45 = "probably" (5)

Table 40: Users preferences for future AEDS tasks (1 = absolutely not, 2 = very improbable, 3 = improbable, 4 = undecided, 5 = probable, 6 = very probable, 7 = absolutely)

This resulted in the following ranking, described in Table 40: Getting a quote from a security company (3.36); Manage personal information items in an AEDS (4.55); Report a theft to the Police (5.00); Inventory important objects or documents (5.00); File a claim with an insurance company (5.45).

It seems that there is a preference for executing standardized processes in an AEDS. This goes along with the observation made from interpreting the item measuring *negotiation power* (see Table 41) based on Liang and Huang's (1998) items as introduced in chapter 5.3.1. Negotiation power refers to the possibility of negotiating terms and conditions.

task	mean	# with experience	mean if experienced	mean if estimated
getting a quote from a security company	3.91	0	-	3.91
file a claim with an insurance company	2.36	3	2.33	2.38
report a theft to the police	2.09	3	1.33	2.38

Table 41: Limitation in negotiation power due to AEDS usage (1 = extraordinarily low, 2 = very low, 3 = low, 4 = identical, 5 = high, 6 = very high, 7 = extraordinarily high)

The task of "getting a quote from a security company" was judged as having identical limitations in negotiation power as perceived in the traditional service delivery (as already experienced or imagined). However, the two other tasks have been judged with a very low degree of limitations in negotiation power when an AEDS is used. Furthermore, we looked more closely at the answers by discerning people that did already experience a real situation (in Table 41, "# with experience) that forced them to reporting a theft or file a claim and "unexperienced" test participants that needed to assume undergoing such a process. As we see, the perceived limitations of negotiation power for filing a claim with an insurance company were nearly rated the same in both groups; the AEDS experience was rated better by people who once have actually had to report a theft to the police. This indicates that users with real-world experience do not feel limited in their negotiation power using an AEDS.

Additionally, we asked how *afraid of getting the wrong product/service* the test subjects were (Table 42), based on the items provided by Liang and Huang (1998). The same pattern emerged as for the limitation in negotiation power: Except for the task "getting a quote from a security" company, the participants expressed less fear when they carried out tasks using an AEDS. This seems suggest the skepticism towards advice-intensive and unknown tasks and their effective execution in an AEDS may exist on behalf of the test subjects.

task	mean	# with experience	mean if experienced	mean if estimated
getting a quote from a security company	4.00	0	-	4.00
file a claim with an insurance company	2.09	3	2.33	2.00
report a theft to the police	1.91	3	1.67	2.00

Table 42: Being afraid of getting the wrong product/service (1 = extraordinarily low, 2 = very low, 3 = low, 4 = identical, 5 = high, 6 = very high, 7 = extraordinarily high)

Furthermore, when we asked the test subjects how *important they value the human component in a business tasks* (an item from Liang and Huang (1998)), again, the unstructured and uncertain task of "getting a quote from a security company" ranged at the top (Table 43) with almost "high".

task	mean	# with experience	mean if experienced	mean if estimated
getting a quote from a security company	4.82	0	-	4.82
file a claim with an insurance company	3.36	3	3.33	3.50
report a theft to the police	3.45	3	2.00	3.88

Table 43: Importance of the human component in business tasks (1 = extraordinarily low, 2 = very low, 3 = low, 4 = identical, 5 = high, 6 = very high, 7 = extraordinarily high)

This supports the interpretation that tasks associated with higher ambiguity are less favored to be executed in an AEDS. Media richness theory (Daft and Lengel 1986) might serve as an explanation for these observations: Textual communication, maybe enriched with pictures, still cannot convey as much information or details that are transmitted in a face-to-face meeting, for example, by giving instant feedback or signaling a real understanding of a problem or situation. The human component was

judged being of "low" importance for the other two tasks. Especially the test subjects who experienced a theft felt less convinced by the human component of a service than those who did not experience such a case before. In the semi-structured interviews, many participants who had to report something as stolen, for instance during their holidays, were rather dissatisfied by the police's performance and the associated waiting times. For this subgroup, lowering the need for human interaction seems to be favorable. During the interviews, many participants noted interestingly that they expect to have more severe difficulties with an insurance company than with the police when they would actually have to execute the tasks in the real-world.

Finally, we asked the participants to rate, in comparison to the conventional process execution as experienced or imagined, how important they judge *initiating business processes at any time* (see Table 44).

task	mean	# with experience	mean if experienced	mean if estimated
getting a quote from a security company	3.64	0	-	3.64
file a claim with an insurance company	4.36	3	4.33	4.50
report a theft to the police	4.45	3	3.33	4.75

Table 44: Importance of initiating business processes any time (1 = extraordinarily low, 2 = very low, 3 = low, 4 = identical, 5 = high, 6 = very high, 7 = extraordinarily high)

The results show, that an AEDS does not fuel the need for carrying out business processes any time. If the test subjects already experienced a theft and have it reported to the police, they were less convinced that they bear the need for initiating a business process at any time (mean = 3.33 = "low") compared to the subjects who have not had this experience (mean = 4.75 = "high"). One can conclude from this observation that after having had an experience with the police, the estimations on their

performance might have decreased or have been too high before thus reflecting exaggerated expectations, for example on the police's capabilities of re-finding something.

To summarize our findings, it seems that citizens and service-providers disliked openly structured or largely unknown business processes which lack prior experience or that require a highly-individualized configuration. This has been observable with the task of getting a quote from a security company. Looking at the interview data, an explanation for this observation can be given: In such open and unknown business processes, the study participants feared to receive the wrong product or the wrong service. Under such circumstances, participants emphasized the need for having a human providing trust and guidance, something which is not necessary in well-known and already experienced form-based business processes such as filing a claim with an insurance company.

> *"Especially the security company, I would like to have personal contact with. With bureaucratic processes, like in an insurance company, I would more readily accept guidance by a program." (P11)*

Furthermore, getting a quote from a security company can be regarded as a service that needs substantial explanatory support for which not every necessary detail can be transmitted via online channels to achieve satisfying results. Thus, such a kind of service falls into the category of delivering experience goods (Girard et al. 2003). It seems unlikely that experience good-like services can be fully supported via intermediaries such as an AEDS; a partial support in less critical transaction phases such as billing might be possible. Because citizens seem to prefer known business process transaction schemes, an AEDS should first provide transactional processes that support self-services which will help to familiarize with an AEDS. Complex services transaction schemes with a higher degree of individualization should be provided later. Summing up, we conclude in **barrier 1:** *Offering unfamiliar services that have a character of experience-goods will be a barrier to an AEDS' adoption.*

5.5.2 Failing to Fulfil Common Service Expectations of the Customers

The participants in the user study complained about having too little information about the current status of a business process they had started because the prototype did not implement such a functionality. The different philosophies for delivering an effective and efficient service can be identified quite prototypically following a traditional private/public sector distinction. *"The claimants want something from us [the Police] – therefore it is their duty to provide correct information."* (police representative) Private sector organizations, such as an insurance company, aim at customer satisfaction: *"Customers should always know about the current status of their case."* (insurance company representative) Therefore, providing status updates comes natural to them. In contrast, the Police as a public sector organization neglects providing such established success factors in e-business (Liu and Arnett 2000) because yet, they did not need to embrace a customer-centric view. This is due to various reasons (resources, strategy etc.). Therefore, we conclude in **barrier 2:** *Not fulfilling common service expectations of the customers will result in a barrier to an AEDS's adoption.*

5.5.3 Failing to Establish Contextual Integrity for Data Sharing

In the user study, the participants raised privacy and security concerns. They wanted to know what happens with their shared data: where is it stored and who can access it? Using a cloud-based service, such as an AEDS, for storing personal information items was criticized and rationalized at the same time. Some participants (five out of twelve) felt generally unsafe having stored personal data in the cloud. One participant framed this feeling of insecurity as follows: *"I would like to control my documents. I would like to know who has access to it. Nobody can guarantee this if I am using Dropbox or SkyDrive. And if it rains, then 'the cloud' has gone. I do not trust them. I use cloud services, but only for insignificant stuff."* (P02) If an end-to-end encryption exists, as stated by a

tech-savvy participant (P12), he would not have any concerns. The service's geographic location was the decisive factor for another participant: *"Probably, I would inform myself before I would use such a service. I would prefer such a service being located in Germany, Switzerland or the European Union."* (P08) Thoughts about security influenced their decision what should be stored in an AEDS and what not. The same participant (and three more of twelve) explained his preference for having a public-sector organization to run an AEDS instead of a private sector company or a start-up company: *"I consider a public authority to be more qualified than a private sector company. With a private company, I feel afraid that they might abuse my data for advertisement or their own purposes because they want to exploit them commercially. That seems less probable with public sector organizations."* (P08) We conclude therefore that creating transparency for information storage and use is an essential design principle for information systems following the user-managed access paradigm. To meet these expectations, already established knowledge of privacy enhancing technologies (Camenisch et al. 2011) must be combined with the process-oriented transaction support in an AEDS. The participants in the user study had concerns where and by whom a service is provided. This observation can be attributed to an individual's aim for keeping "contextual integrity", a concept developed by Nissenbaum (2010). Therein, information items can be shared guided by norms of appropriation and distribution tied to a certain context. The context is formed by the source, destination and the appropriateness of the content. By exerting control and having transparency, people are able to maintain contextual integrity. This point of view also gains momentum in other areas of research, such as HCI (Barkhuus 2012). We, therefore, conclude in **barrier 3**: *Failing to establish contextual integrity will cause a barrier to the adoption of an AEDS.*

5.5.4 Failing to Establish and Run a Multi-Sided Platform

Taking the customer perspective, the study participants generally recognized the advantages of creating and receiving information items digitally and their re-use in digital business processes. Having everything at

one place and being able to forward information items was judged by nearly all (nine out of twelve) participants as something positive and beneficial: *"Forwarding things, for instance to the Police or to an insurance company, would not have been possible with my system [Dropbox]."* (P09) Another participant stated, that if he had all his digital belongings and documents organized neatly in an AEDS, he would not like to suffer from a vendor lock-in. The information items as well as all the effort to organize them should not be lost when, due to some reason, a change of the AEDS provider is necessary. Looking at the service-providers, a mixed picture arises: In general, the police representative was critical about the current prototype. Without a deep integration into the Police's back-end systems (which has not been done in the prototype), he concluded that the AEDS prototype only brings advantages to the citizen and not to him. The insurance company representative was convinced by the concept of an AEDS and its prototypical implementation but wondered about the need for critical mass: *"If the usage numbers are big enough, such a concept would be beneficial to us. The problem is to motivate a substantial number of our customers to use such a tool to achieve enough usage."* (insurance company representative)

To summarize, an AEDS as a multi-sided platform faces challenges to find a suitable business model that satisfies all relevant stakeholders: (a) the AEDS platform provider, (b) the service-providers from the private and public sector that offer services using the AEDS platform, and (c) the customers willing to engage in business transactions and/or store personal information items. Attracting a sufficient number of customers and service-providers, which is vital for a network good, resembles the well know chicken-and-egg problem. In a free market, where many AEDS platform providers compete for customers, they need to differentiate by offering "value-added" services going beyond the simple storage of information items (Pfister and Schwabe 2013). For example, individuals can be supported in their personal information management by breaking down larger information organizing tasks into smaller tasks that can be worked upon using different devices at different locations, for instance, tagging photos and grouping them into galleries. This strategy is called

"Selfsourcing" (Teevan et al. 2014). It could be complemented for specific tasks with the concept of crowd sourcing which served as the original inspiration for the selfsourcing concept. We summarize these challenges in **barrier 4:** *Failing to establish and run an AEDS as a multi-sided platform with an attractive business model will be a barrier for the adoption amongst all stakeholders.*

5.6 Potential Benefits and Challenges

5.6.1 Potential Benefits

Using the willingness-to-pay and a task's attractiveness as indicators for potential benefits on behalf of the customers/citizens, we conclude that:

- AEDS reduce the perceived efforts to control one's data,
- WTP is higher for complex tasks and for assistive tasks related to inventorying and keeping an overview of one's personal data,
- archival tasks (collecting documents, capturing receipts and bills) are likely to be outsourced instead of carrying them out yourself,
- controlling and creatively answering requests are tasks which clearly want to be performed by the test subjects/AEDS users themselves,
- answering requests with an AEDS seems to be an acceptable "new" channel for the test participants.

These findings are congruent with the observations from the customer/client perspective based on the qualitative interviews. For instance, the test participants generally uttered positive impressions about the AEDS prototype and expressed a favor for structured processes.

Moreover, the combination of information items generated in advisory sessions (crime prevention) which can be re-used in business processes and transactions within an AEDS were judged as very positive by our test participants.

5.6.2 Challenges and Design Implications

5.6.2.1 Citizen/Customer Perspective

Nevertheless, some challenges could be discovered on the *citizen/client perspective* that need to be addressed adequately in the design of an AEDS and its functionalities. Therefore, we suggest initial design implications to address the identified challenges.

1. The mobile app was preferred to capture photos and short information snippets. Writing longer passages of text or doing more cognitive demanding work with an information item is preferably done with a stationary device such as a laptop having a bigger screen and maybe a pointing device such as a mouse.

   Suggested design implications:
   a) Empower a user to smoothly transition between different devices.
   b) Provide device-independent functionalities for accessing, creating, and editing information items.

2. Populating an AEDS with information items was identified as an obstacle for the acceptance and usage of such a tool. Moreover, the discipline to keep information items continuously updated was judged as very likely to become a problematic issue in the future.

   Suggested design implications:
   a) Assist users in initially populating an AEDS by providing import functions for existing data and templates reducing the individual user's efforts.
   b) Assist users in capturing metadata by using existing data bases that can be consulted to minimize own efforts, for example, by only adding a unique serial number instead of describing generic details of a product that could have been imported.

c) Motivate and incentivize users to keep their information items updated using approaches such as gamification, intelligent assistants and/or reminders.

3. Security fears were omnipresent. The test participants were aware of the sensitive nature of the information items that could be stored in an AEDS and were unison concerned about security. But, as already diagnosed as the privacy paradox (Norberg et al. 2007; Pavlou 2011), some participants still acted in another manner than they described they wanted or aspired to. Getting hacked was the major concern which was uttered by the test participants.

   Suggested design implications:
   a) Use encryption and explain the preventive measures taken. This creates transparency.
   b) Help users to decide if they want to store information items in an AEDS by providing them understandable explanations how the service works and protects their data.

4. Our test participants simultaneously expressed their favor and a kind of fear for structures and structured processes. Nevertheless, when information items needed to be exchanged, the test participants felt uncertain how the information items attached to a business transaction were handled. This is largely due to the design of the prototype, but these concerns need to be addressed in a product version of an AEDS.

   Suggested design implications:
   a) Transaction handling with an AEDS must be designed in such a way that users do not feel incapacitated or paralyzed by too much automation. On the other hand, too much involvement or need for confirmation might also be counterproductive.
   b) If information items need to be attached to business processes in transactions, the status of an information item must be

made clear: is it a reference to something stored in an individual's AEDS or is it a copy (to allude to a concept in programming: is it a call-by value or a call-by reference). This must be made transparent besides the transparency with whom information items are shared.

5.6.2.2 Service Provider Perspective

Now, we switch to the perspective of the *service providers* who painted a rather mixed picture when they reported upon the experiences with the AEDS prototype. On the one hand, business drivers such as cost reduction and speeding up transactions were evident and welcomed. On the other hand, problematic areas were identified. Besides the barriers to t-government presented in the previous chapter, some other challenges were raised or made obvious due to the exploratory evaluation of the AEDS prototype. They were predominately related to data quality, either of metadata or photos.

1. Especially the police representative remarked that unique identifying properties need to be captured in order to really describe an object. This is related to the challenges on the customer's side to provide details and seize plenty of input data.

   Suggested design implications:
   a) As it has been already proposed for the clients, the support in capturing information items must be automated as much as possible to incentivize customers to really provide the unique information that is needed, for example, when an object has to be reported as stolen.
   b) On the client's side, the results from the WTP also indicate that some tasks exist that people would pay for to have them done – which opens up new possibilities for designing supporting tools and services around such tasks.

2. The role of photos as proofs or the way they are captured therefore has to be reconsidered due to substantial improvements that could be achieved compared to the pictures that were taken during the explorative evaluation. According to the police representative, a certain level of quality and details is needed to provide the level of details (showing unique characteristics or identifiers) that is needed for a successful description to search for these objects.

   Suggested design implication:
   If physical objects should be captured as electronic photos, the owner of the objects should be supported in taking "relevant" pictures (from several angels, providing details, and indicating the size of an object using a reference scale for estimating dimensions). Additionally, a kind of intelligent "quality checker" or smart assistant for taking such pictures could be envisioned, too.

3. The different organizations taking part in the evaluation had very different approaches, habits and principles how to deliver their services to their citizens or customers. For example, the security company favored a very individualized on-site approach whereas the insurance company tried to streamline its processes to optimize them for mass market service delivery aiming at minimizing personnel intense contact with customers due to the costs this generates. Public authorities do also offer a wide spectrum of service delivery habits.

   Suggested design implication:
   This spectrum of expectations, habits and visions of service delivery and interaction need to be addressed by appropriate support with an AEDS. The support levels are ranging from simple document reception or sending to enable transactions. If the trend towards service dominant logic continues and value co-creation prevails, AEDS providers need to onboard and convince organizations with business plans and functionalities that also support a service provider's transition into a co-creation-based service-delivery mode.

5.7 Discussion

In order to categorize the four barriers that have been elaborated in chapter 5.5, we argue for the creation of a new, "citizen-oriented service design" category. The four newly discovered barriers as well as the potential benefits and challenges do neither resemble impediments on the governance, organizational or managerial or technological level as categorized by Veenstra et al. (Veenstra et al. 2011). Nor can they be understood as "organizational and social" challenges within an organization, a category used by Weerakkody et al. (Weerakkody et al. 2008). The character the four barriers share is related to the citizens, their service expectations, needs or fears. Therefore, we suggest to summarize these four barriers under the new category "citizen-oriented service design" (which also should encompass "customer-oriented service" design if the domain of reference is e-business in contrast to e-government). Reflecting upon the newly discovered barriers contributes to the design of AEDS and to t-government at the same time which will be discussed in the following sections in order to wrap up the findings of this essay.

Electronic data safes have the potential to help citizens in overcoming the problem of information fragmentation. The ability to interact with business processes transforms electronic data safes into active electronic data safes. Certainly, these tools provide more capabilities for information sharing under the user-managed access paradigm than ordinary portals or electronic data safes. Nevertheless, they will face challenges related to the governance, organizational or managerial, technological or social level. But our results also indicate that the service design needs to pay attention to the individuals as users or customers of an AEDS. Using the perspective of a "citizen-oriented service design", we interpret our findings as a call to action to come up with research to identify further barriers and challenges that are related to the citizens and customers who make use of new technologies and services. In doing so, the following question can be answered to shape new services before they are rolled out: With respect to a new service delivery paradigm, such as an AEDS, which character of services do citizens or customers favor under which

conditions? The potential benefits and challenges with the suggested design implications (chapter 5.6) can be seen as a first attempt to clarify this question. Furthermore, the design implications can be used to help defining requirements for system design.

T-government can benefit from integrating the citizen-/customer-oriented service design perspective, too, in order to develop solutions that are truly citizen-centric. As our example with an exploratory study of an AEDS has shown, innovations or new technologies to support t-government need to bring utility not only to the organization but also, and foremost, to the citizen as service users. Thus, they need to have a satisfying degree of maturity. Therefore, we conclude that an assessment of t-government readiness from a user-perspective needs to be integrated in the discussion of future barriers. As an important side product of a user-centric evaluation, other potential benefits, challenges or even requirements can be identified, too (as performed in chapter 5.6). Instead of just looking back on what went wrong after new services and technologies have been launched, t-government research should take an active stance to identify unknown barriers and challenges ahead. User studies in a quasi-realistic setting seem promising to achieve this.

5.8 Limitations

As a limitation to this study, the participants in the user study do not reflect a representative part of the population, and the number of service providers might seem too limited and narrow to come up with results having a high internal validity and, thus, not being fruitful for generalization. Nevertheless, (single) case studies produce rich observations and propositions can be derived from all observations helping to guide further theory development, for example, by pointing to new research challenges that arise and would not have been found otherwise. This argument reflects this article's exploratory approach. Furthermore, the tasks in the user study were purposefully chosen to cover realistic problems and that the participants could work in a nearly realistic setting.

5.9 Conclusion

In this essay, we identified four new impediments or barriers related to an AEDS when such a tool is used to support t-government by offering a technical solution to put the paradigm of user-managed access into practice in order to overcome data silos: 1.) offering citizens unfamiliar services having the character of experience-goods; 2.) failing to fulfil common service expectations of the customers; 3.) failing to establish contextual integrity for data sharing; 4.) failing to establish and run a multi-sided platform. Furthermore, potential benefits and challenges, as well as possible design implications which could serve as input for requirements have been identified, too.

Without our exploratory approach involving a user study with a prototype, those findings would not have been identified. Therefore, we argue that t-government projects benefit from early prototyping and evaluation with all relevant stakeholders in order to avoid misconceptions leading to unusable and unaccepted solutions. User-centered design methods and design science research (Hevner et al. 2004) help to uncover "hidden" assumptions or problematic areas. Applying such methods and paradigms helps to understand better specific contexts but they may also generate transferable knowledge for other contexts or domains.

The study participants welcomed the concept of an AEDS helping them in organizing their administrative burdens. This gives confidence that the concept of an AEDS and its underlying user-managed access paradigm will fall on fertile grounds. Nevertheless, further research is needed to come up with solutions that tackle the newly identified and existing barriers to t-government as well as translating the identified potential benefits and challenges into requirements.

6 Outlook: EDS as an Infrastructure for Smart Interactions

This chapter relates and integrates the findings that were elaborated in the previous essays in a coherent discussion related to possible future prospects of a smart government and smart business a.k.a. industry 4.0.

Smart cities are an emerging topic although the term "smart" is used very broadly in its widest sense meaning "intelligent" but no commonly accepted definition exists for smart cities. Using information and communication technology (ICT) helps to efficiently manage many dimensions of a smart city, for example, mobility, governance, environment etc. which will in turn bring benefits to the citizens and contribute to achieve the overall aim of reducing resource consumption. (Castelnovo 2016)

Von Lucke (2015) gives an overview of the use of the adjective "smart" in different contexts and provides an overarching definition of smart objects as *intelligently networked objects* and services using ICT. In his works (von Lucke 2015, 2016a, 2016b), von Lucke introduced the term "smart government" and defined it, in close relation to the definition of industry 4.0 (acatech and Promotorengruppe Kommunikation der Forschungsunion Wirtschaft-Wissenschaft 2013), as follows (visualized in Figure 12): *"Smart Government should be understood as the management of business processes related to government and administration with the help of intelligently networked information and communication technologies (ICT). Intelligently networked governance uses the opportunities of interconnected smart objects and cyber-physical systems for the efficient and effective performance of public tasks. This includes the portfolio of e-government and open government, embracing big data and open data. At its core, it is about sustainable government and administrative actions in the age of the Internet of Things and the Internet of Services, whose technical foundation is on the Internet of Systems, the Internet of People and the Internet of Data. This definition includes the local or municipal level, the regional or provincial level, the national or federal level as well as the*

supranational and global level. Included is thus the entire public sector, consisting of legislative, executive and judiciary as well as public enterprises." (von Lucke 2016a, p. 139)

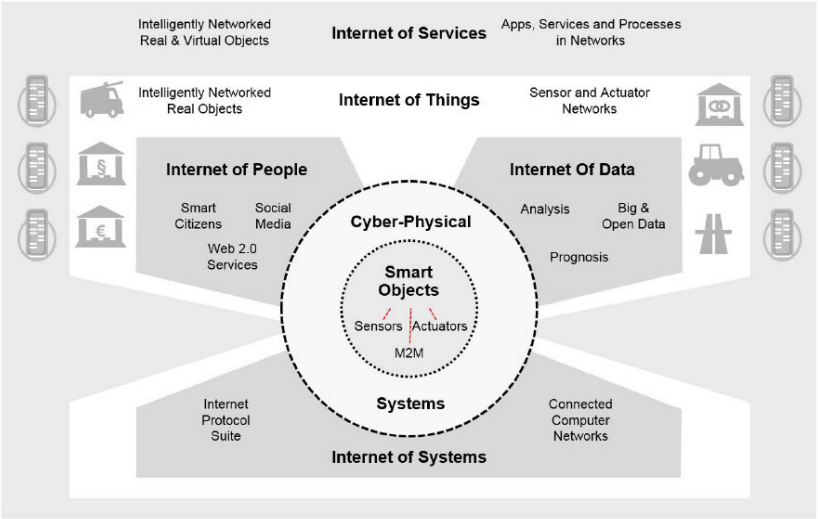

Figure 12: Constituting elements of Smart Government (von Lucke 2016a, p. 139)

Cyber-physical systems are complex systems of intelligently connected real-world and virtual objects that "[...] gather data, analyze it and initiate task execution for which they use interconnected smart objects, embedded systems or sensor networks." (von Lucke 2016a, p. 137) They are assumed to have substantial effects on politics, administration and society in the future – something which is also aimed for with the concept of transformational government as an abstract aim (see chapter 5.2.1 on page 179) and these cyber-physical systems might contribute to achieve these goals. Von Lucke (2016b, p. 175) also proposed a stage model for the evolution of the Internet and the World Wide Web (see Table 45) which helps to better understand the constituting elements of this "smart government". The Internet of Things and Services with cyber-

physical systems (as the Web 4.0) sits on top of all other layers and uses the technology provided by the lower-level stages.

Web 5.0	Tactile Internet	Real-time networked communication	Real-time Government
Web 4.0	Internet of Things & Internet of Services	Smart objects, Cyber-physical systems	Smart Government
Web 3.0	Internet of Data Semantic Web	Linked Data, Open Data, Big Data, Big Data Analytics	Open Government Data
Web 2.0	Internet of People Social Web	Networked communication using social media	Open Government
Web 1.0	Internet of Systems World Wide Web	Networked communication using the World Wide Web	Electronic Government

Table 45: "Häfler" (Friedrichshafener) Stage model for the evolution of the Internet and the World Wide Web (von Lucke 2016b, p. 175)

Now, the question arises, how electronic data safes fit into the landscape of smart services and smart government. In his whitepaper introducing the notion of smart government, von Lucke (2015) claims that people as citizens need to decide themselves and that they should not be dictated by fully-automated systems and processes. Electronic data safes can help to achieve this aim by following the user-managed access paradigm and seeing an EDS as a technological tool to exert informational self-determination. Because the EDS owners decide with whom they want to share information items, they keep control over their data. An EDS could serve

as a kind of cockpit for all information items and processes that are related to a citizen thereby empowering individuals by giving them (back) control. The information items that are stored in an EDS might be hybrid documents that are readable by humans and machines at the same time thus spanning the Web 1.0 to the Web 4.0 as introduced by von Lucke. Furthermore, if sensory data of smart objects needs to be stored, an EDS might also serve as convenient storage location which reflects the hierarchical service layers for EDS as introduced as a finding in chapter 2.5 on page 69). By adding value-added services such as individualized statistics, sensory raw data will be transformed into understandable information items that can be re-used in business processes on the top layer. With user-managed access as the leading design principle, such data collections and their (re-)use give back control to the individual as the owner. This vision of controlling and managing important facets of an individual's personal data are also reflected in the visions of life-management platforms (Kuppinger and Kearns 2013; or visualized in a video by Siegel 2011) or, on a more general level, how the Semantic Web could transform business (Siegel 2009). The findings elaborated in essay three of this thesis, notably the sensitizing concept of the data value zones, might help to design functionalities that support the fine-grained sharing of information items in an EDS respecting the usage-patterns and habits that have been emerging – which ultimately fosters an EDS's adoption and (commercial) success.

As another advantage of the Internet of Services, von Lucke (2015) suggests that instead of making objects more intelligent, the processing of data will be moved "in the cloud" or the Internet of Services to achieve added value. For example, an EDS could also be used to store health-related information items of an individual (maybe self-disclosed by using fitness trackers or as results of medical examinations). By sticking to the user-managed access paradigm, an individual maintains control over this sensitive data in an EDS. But if individuals as data owners chose to share data anonymously to support Big Data analytics in the health domain, an EDS could provide the technological support for doing this – creating

benefits for the individual and the society as well. In opening up and contributing information items, individuals do have the possibility to act as co-producers of services. This aim of citizens being enabled to act as co-producers (for public services) was described by Castelnovo (2016) which entails the need for government to re-think its role as "organizer, enabler, and catalyst of the efforts of individuals and groups" (Castelnovo 2016) – or, to put it into other words: to become smart. Smart e-business and e-government processes, if they are fully digitized, are advantageous because no changes in media occur which opens up new possibilities for citizen or customer co-production and process optimizations in the public or private sector.

Electronic data safes can be interpreted as a customer-centric interface connecting the Internet of Things, the Internet of Services with the Social Web, the Semantic Web and the World Wide Web (in reference to von Lucke's proposed stage model introduced before). Based on this technological tool, citizens can evolve as co-producers opening up an evolution of value creation processes as described by Castelnovo (2016) and visualized in Table 46.

		Responsibility for design of public services		
		Public servant	**Public servant and clients citizens**	**Clients/Citizens**
Responsibility for delivery of public services	**Public servant**	1. Traditional service provision	2. Mixed (co-production on design side)	3. Public servant as a sole deliverers
	Public servant and clients citizens	4. Mixed (co-production on the delivery side)	*5. Full co-production*	6. Mixed (co-production on the delivery side)
	Clients/Citizens	7. Clients/citizens delivery of a professionally designed service	8. Mixed (co-production on design side)	9. Self-organized client/citizens provision

Table 46: Roles in co-production (Castelnovo 2016)

The path between configuration 1 and configuration 9 reflects the progression of the power relationships between citizens and authorities/organizations. This path of development also reflects the ladder of citizens' participation (Arnstein 1969) which has three stages: Non-Participation, Tokenism and Citizen Power. Tokenism "[...] allows the have-nots (citizens) to hear (Informing), have voice (Consultation) and advise, although the power-holders retain the right do decide (Placitation). Finally, in the stage of Citizen Power, citizens can engage in trade-offs with power-holders (Partnership), obtain the dominant decision-making authority in a plan or program (Delegated Power), or full managerial power (Citizen Control)." (Castelnovo 2016) Keeping these roles of co-production in mind, an EDS has the potential to serve as an infrastructure to realize the vision of a smart government – and smart business with respect to industry 4.0 which is also using cyber-physical systems and the Internet of Things and the Internet of Services to modernize value creation in the future as a kind of fourth industrial revolution (after mechanization, mass production, and automation). As diagnosed in the analysis of business models for EDS (see chapter 2.4 on page 57), successful EDS solutions, such as the Danish E-Boks, transcend sectoral usage by bridging the public sector and the private sector as well delivering true value for individuals using an EDS by reducing information fragmentation. Furthermore, EDS services need to become horizontally integrated solutions that tackle problems and challenges of personal information management and process integration as a whole from a user-centered perspective to realize true benefits instead of piecemeal progress. The concept of EDS has the potential to contribute to disruptive changes instead of just providing insignificant evolutionary steps.

In the following, a SWOT (Strengths – Weaknesses – Opportunities – Threats) analysis will be used to identify an EDS's potential with respect to a future facing an evolution towards smart government and industry 4.0 (see Table 47).

Strengths	Weaknesses
▪ User-managed access as the leading design principle ▪ Reducing and avoiding information fragmentation due to an EDS' role as a hub for managing personal information items. ▪ Supporting individuals in managing their "contractual" relationships and digital presence. ▪ Applicability of an EDS in cross-sectoral (G/B2C) tasks, even with sensitive data (for example, health-related data).	▪ Chicken or egg dilemma of incentivizing development in the private or public sector due to inexistent or unclear demand ▪ Initial funding for development ▪ Viable business model ▪ Individuals might judge constant decision-taking due to the user-managed access paradigm as too bothersome over time. ▪ Interoperability of data and processes based on technological and business-related issues.
Opportunities	**Threats**
▪ Ongoing trend towards digitization of services fosters the need for new solutions for storage and support, for example, due to innovative cyber-physical systems ▪ Potential of an EDS to serve as a customer-oriented façade for smart government and industry 4.0 (data-intensive) services. ▪ Innovation potential due to creating "value added" or "process support" services on top of an EDS's storage layer. ▪ Cost and fee reductions ▪ Mass customization of processes	▪ Fear of service providers of giving away their unique point of contact (own portals) to a more generic EDS. ▪ Security threats due to an EDS's character as a hub so that it could become the preferred target for hacking information items ▪ Lack of funding ▪ Lack of acceptance because of poorly designed digital practices that may not reflect (culturally enacted) practices of sharing information items (while living and beyond an individual's death).

Table 47: SWOT analysis of EDS with respect to smart government and industry 4.0

The *strengths* of an EDS are predominately related to its leading design principle of user-managed access. This powerful paradigm allows users to decide, which information items are shared with whom or with which processes. Having such a tool at hand gives back control to individuals over their personal information items which forms part of a future-oriented personal information management. Furthermore, by concentrating all important information items at one spot or having a kind of directory where such information items are located, an EDS helps to reduce or even overcome the problem of information fragmentation. Individuals are given a technological tool at hand to manage their "official and administrative life" which opens up possibilities for a future service design focusing on value co-creation which might be only possible or positively supported by the user-managed access paradigm. And, last but not least, the EDS concept shows great potential to be applicable in cross-sectoral interactions when individuals interact with "official", governmental organizations as well as private-sector organizations and all information items are stored or exchanged via an EDS as a hub. Taken together with the user-managed access paradigm, an EDS concept is agnostic to which kind of information items are stored and shared in there – which could also be easily extended to sensitive data or information items, for example, health-related data from fitness trackers or even medical reports.

There are also many *opportunities* indicating that an EDS may become an indispensable tool in the future due to external factors triggered by economic and political developments. For instance, there is the ongoing trend of digitizing services which will ultimately create a need to store and share these digital information items. Due to the rise of intelligently networked cyber-physical systems, the amount of individually created sensory data needs to be stored somewhere and – for the benefit of the individual or the users/society – sharing on a user-managed access basis seems to be a viable option to create services bringing added-value to the data owners. Therefore, an EDS seems to have the potential to serve as a customer-facing interface to integrate personal information items with smart government or industry 4.0 processes. Instead of creating islands

of isolated services, interconnected services and data seems to be a necessity. But the current infrastructure of personal information management tools does not provide such integrative tools – which should be interpreted as a call for action on behalf of all stakeholders (service providers, EDS platform providers, and individuals). By offering value-added services to the data owners and capabilities of process support, a huge potential of innovations could be unleashed. As very plausible opportunities, that speak for the implementation of the concept of an EDS in smart government and e-business, are the obvious advantages of cost or fee reductions. They might even lead to more individualized services resulting in a kind of mass customization of individualized processes. These opportunities promise clear benefits for the service providers and the individuals as customers or users of an EDS.

But there are also *weaknesses* associated with the concept of an EDS. The biggest challenge is to solve the chicken or egg dilemma: EDS platforms can only thrive if enough service providers would connect to them – and vice, versa, service providers would only like to join EDS platforms that already thrive. This is evident for the public sector as well as for the private sector when user-side demand and ultimately an EDS's adoption is not clearly predictable which would be desirable before investments in EDS developments are undertaken. The initial funding for the EDS development is a huge problem and relates to the open question who should better run such a service: the public or the private sector? Another weakness is to find a viable business model to keep an EDS constantly funded. On the user-side of an EDS, one weakness might be the constant need to take decisions which information items should be shared with whom due to the user-managed access paradigm. This might become too bothersome for individuals in the future. The challenge will be to design an EDS and services using an EDS in such a way that smart individuals are smartly supported to take these decisions without just clicking "yes" to everything resembling a kind of unreflective "nodding with the head" just to have peace of mind (or less notifications in one's EDS). Another weakness is the need for technological interoperability of data and processes that are interconnected via an EDS and the service providers. A

data exchange on a syntactic level seems fairly achievable but to agree upon semantics of data and data quality standards to use these information items in automated processes will be a future design challenge – as it is already observable in B2B interactions using, for example, web services and an enterprise service bus as underlying technology. Particular business-interests may place additional hurdles on the automated information item exchange based on user-managed access that need to be successfully addressed in order not to remain a weakness.

As *threats* to the concept of EDS, several external factors can be identified. First, they are related to the nature of the service providers not wanting to give away their unique point of contact with their customers to a more generic EDS. This threat needs to be addressed by functionalities and governance mechanisms that appease the service provider's fear of losing their direct contact with customers. The threats to the realization of smart government and industry 4.0 with an EDS as an infrastructure component is related to its character as a monolithic and centralized hub where really everything valuable about an individual could be stored. Security threats of getting hacked, data fraud, or data leakage need to be addressed from all stakeholders in a convincing technological and educational manner to give individuals a true picture about the benefits and dangers they might be confronted using an EDS – and maybe additional advice how to reduce risks in order to foster trust. Another threat is the lack of funding for the initial development and the continuing operations of an EDS. Moreover, if services are not designed in a user-centric fashion respecting the culturally enacted practices of sharing information items, there is the real threat of non-adoption by potential users. Especially practices surrounding sharing information items in a relationship or family context need to be taken into account for the design of services with respect to an individual's life-time and beyond.

In sum, electronic data safes do have great potential for becoming an infrastructure for disruptive changes in the era of smart government and industry 4.0.

7 References

acatech, and Promotorengruppe Kommunikation der Forschungsunion Wirtschaft-Wissenschaft. 2013. "Deutschlands Zukunft als Produktionsstandort sichern. Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0," (available at http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Abschlussbericht_Industrie4.0_barrierefrei.pdf).

accenture. 2011. "Achieving High Performance in the Postal Industry," Accenture Research and Insights (available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-High-Performance-Postal-Industry-2011-Final.pdf).

Acker, A., and Brubaker, J. R. 2014. "Death, Memorialization, and Social Media: A Platform Perspective for Personal Archives," *Archivaria* (77), pp. 1–23.

Allen, D. 2001. *Getting things done: the art of stress-free productivity*, London: Penguin Books.

AlSoud, A., and Nakata, K. 2011. "A conceptual life event framework for government-to-citizen electronic services provision," *ICIS 2011 Proceedings* (available at http://aisel.aisnet.org/icis2011/proceedings/servicescience/7).

Andrieu, J. 2010. "The Information Sharing Report," Work Group Report, Kantara Initiative (available at http://www.projectliberty.org/confluence/download/attachments/44564807/The+Information+Sharing+Report.Work+Group+Report.pdf).

Arnstein, S. R. 1969. "A Ladder Of Citizen Participation," *Journal of the American Institute of Planners* (35:4), pp. 216–224 (doi: 10.1080/01944366908977225).

Ates, M., Ravet, S., Ahmat, A. M., and Fayolle, J. 2011. "An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and Other Delights," in *Sixth International Conference on Availability, Reliability and Security (ARES)*, Presented at the Sixth International Conference on Availability, Reliability and Security (ARES), IEEE, August 22, pp. 555–560 (doi: 10.1109/ARES.2011.85).

Badger, M. L., Grance, T., Patt-Corner, R., and Voas, J. M. 2012. "Cloud Computing Synopsis and Recommendations," No. NIST SP-800-146, (available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=911075).

Banks, R. 2011. *The Future of Looking Back*, Microsoft Press.

Banks, R., Kirk, D., and Sellen, A. 2012. "A Design Perspective on Three Technology Heirlooms," *Human–Computer Interaction* (27:1–2), pp. 63–91 (doi: 10.1080/07370024.2012.656042).

Bannister, F. 2001. "Dismantling the silos: extracting new value from IT investments in public administration," *Information Systems Journal* (11:1), pp. 65–84 (doi: 10.1046/j.1365-2575.2001.00094.x).

Barkhuus, L. 2012. "The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 367–376 (doi: 10.1145/2207676.2207727).

Barth, M., and Veit, D. 2011. "Electronic Service Delivery in the Public Sector: Understanding the Variance of Citizens' Resistance," Presented at the 2011 44th Hawaii International Conference on System Sciences (HICSS), January, pp. 1–11 (doi: 10.1109/HICSS.2011.181).

Beaudry, A., and Pinsonneault, A. 2005. "Understanding User Responses to Information Technology: A Coping Model of User Adaptation," *MIS Quarterly* (29:3), pp. 493–524.

Berg, B. L. 2007. *Qualitative research methods for the social sciences* (6th ed.), Boston: Pearson/Allyn & Bacon.

Berger, J. B. 2014. "Mandatory e-government has arrived: The silent protest from staff calls for the committed scholar–resistance must never be futile!," in *The 25th Australasian Conference on Information Systems, ACIS 2014*, ACIS (available at http://hdl.handle.net/10292/8115).

Berger, J. B. 2015. "E-government harm: An assessment of the Danish coercive Digital Post strategy," Roskilde University (available at http://forskning.ruc.dk/site/services/downloadRegister/55545118/PHD_050615_v3_final_publication_1_Berger.pdf).

Berger, J. B., and Hertzum, M. 2014. "Adoption Patterns for the Digital Post System by Danish Municipalities and Citizens," in *Proceedings of the European Conference on Information Systems (ECIS)*, Presented at

the ECIS, Tel Aviv, Israel (available at http://ecis2014.eu/E-poster/files/0558-file1.pdf).

Bergman, O., Beyth-Marom, R., and Nachmias, R. 2006. "The project fragmentation problem in personal information management," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, New York, NY, USA: ACM, pp. 271–274 (doi: 10.1145/1124772.1124813).

Bergman, O., Whittaker, S., Sanderson, M., Nachmias, R., and Ramamoorthy, A. 2010. "The effect of folder structure on personal file navigation," *Journal of the American Society for Information Science and Technology* (61:12), pp. 2426–2441 (doi: 10.1002/asi.21415).

Bharosa, N., Janssen, M., Klievink, B., and Tan, Y. 2013. "Developing multi-sided platforms for public-private information sharing: design observations from two case studies," in *Proceedings of the 14th Annual International Conference on Digital Government Research*, ACM, pp. 146–155 (available at http://dl.acm.org/citation.cfm?id=2479747).

Blevis, E., Bødker, S., Flach, J., Forlizzi, J., Jung, H., Kaptelinin, V., Nardi, B., and Rizzo, A. 2015. "Ecological Perspectives in HCI: Promise, Problems, and Potential," in *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA '15, New York, NY, USA: ACM, pp. 2401–2404 (doi: 10.1145/2702613.2702634).

Bloching, B., Luck, L., and Ramge, T. 2012. *Data Unser: Wie Kundendaten die Wirtschaft revolutionieren*, München: REDLINE.

Blomberg, J., and Karasti, H. 2013. "Reflections on 25 Years of Ethnography in CSCW," *Computer Supported Cooperative Work (CSCW)* (22:4–6), pp. 373–423 (doi: 10.1007/s10606-012-9183-1).

Boardman, R., and Sasse, M. A. 2004. "'Stuff goes into the computer and doesn't come out': a cross-tool study of personal information management," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, New York, NY, USA: ACM, pp. 583–590 (doi: 10.1145/985692.985766).

Bødker, S., and Klokmose, C. N. 2012. "Dynamics in Artifact Ecologies," in *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*. NordiCHI '12, New York, NY, USA: ACM, pp. 448–457 (doi: 10.1145/2399016.2399085).

Böhmann, P. D. T., Leimeister, P. D. J. M., and Möslein, P. D. K. 2014. "Service Systems Engineering," *Business & Information Systems Engineering* (6:2), pp. 73–79 (doi: 10.1007/s12599-014-0314-8).

Borgmann, M., Hahn, T., Herfert, M., Kunz, T., Richter, M., Viebeg, U., and Vowé, S. 2012. "On the Security of Cloud Storage Services," No. SIT-TR-2012-001, Darmstadt: Fraunhofer Institute for Secure Information Technology SIT (available at http://www.sit.fraunhofer.de/content/dam/sit/en/studies/Cloud-Storage-Security_a4.pdf).

Braun, V., and Clarke, V. 2006. "Using thematic analysis in psychology," *Qualitative Research in Psychology* (3:2), pp. 77–101 (doi: 10.1191/1478088706qp063oa).

Breidert, C., Hahsler, M., and Reutterer, T. 2006. "A review of methods for measuring willingness-to-pay," *Innovative Marketing* (2:4), pp. 8–32.

Breitenstrom, C., Brunzel, M., and Klessmann, J. 2008. "Elektronische Safes für Daten und Dokumente," White Paper, Berlin: Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS) (available at http://www.fokus.fraunhofer.de/de/elan/_docs/_hpp-gruppe/esafe_white-paper_081219.pdf).

Brenner, W., Karagiannis, D., Kolbe, L., Krüger, J., Leifer, L., Lamberti, H.-J., Leimeister, J. M., Österle, H., Petrie, C., Plattner, H., Schwabe, G., Uebernickel, F., Winter, R., and Zarnekow, R. 2014. "User, Use & Utility Research: The Digital User as New Design Perspective in Business and Information Systems Engineering," *Business & Information Systems Engineering* (6:1), pp. 55–61 (doi: 10.1007/s12599-013-0302-4).

Briggs, R. O., and Schwabe, G. 2011. "On Expanding the Scope of Design Science in IS Research," in *Service-Oriented Perspectives in Design Science Research*. Lecture Notes in Computer Science, H. Jain, A. P. Sinha, and P. Vitharana (eds.), Springer Berlin Heidelberg, pp. 92–106 (available at http://link.springer.com/chapter/10.1007/978-3-642-20633-7_7).

Brochot, G., Brunini, J., Eisma, F., Larsen, R., Lewis, D. J., and Zhang, J. 2015. "Study on Personal Data Stores conducted at the Cambridge University Judge Business School," *Study on Personal Data Stores conducted at the Cambridge University Judge Business School*, August 7

(available at https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school; retrieved December 22, 2016).

Brubaker, J. R. 2013. "The Afterlife of Identity," in *Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion*. CSCW '13, New York, NY, USA: ACM, pp. 39–42 (doi: 10.1145/2441955.2441967).

Brubaker, J. R., and Callison-Burch, V. 2016. "Legacy Contact: Designing and Implementing Post-mortem Stewardship at Facebook," Presented at the CHI 2016, San Jose, CA, USA: ACM Press, pp. 2908–2919 (doi: 10.1145/2858036.2858254).

Brubaker, J. R., and Hayes, G. R. 2011. "'We Will Never Forget You [Online]': An Empirical Investigation of Post-mortem Myspace Comments," in *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*. CSCW '11, New York, NY, USA: ACM, pp. 123–132 (doi: 10.1145/1958824.1958843).

Brubaker, J. R., and Vertesi, J. 2010. "Death and the social network," in *Proc. CHI Workshop on Death and the Digital* (available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.167.7578&rep=rep1&type=pdf).

Brucker-Kley, E., Keller, T., Kurtz, L., Pärli, K., Pedron, C., Schweizer, M., and Studer, M. (n.d.). "Passing and Passing on in the Digital World," in *Proceedings of the IADIS International Conference on e-Society*. P. Kommers and P. Isaias (eds.), Presented at the e-Society Conference, Portugal, pp. 248–256 (available at http://www.esociety-conf.org/ebooks/201301L032.pdf).

Brunzel, M. 2011. "Intermediäre Geschäftsmodelle an den Schnittstellen zur öffentlichen Verwaltung," in *Bürokratieabbau im Verwaltungsvollzug: Better Regulation zwischen Go-Government und No-Government*E-Government und die Erneuerung des öffentlichen Sektors, M. Brüggemeier and K. Lenk (eds.), Berlin: Edition Sigma, pp. 125–134.

Brush, A. B., and Inkpen, K. M. 2007. "Yours, mine and ours? Sharing and use of technology in domestic environments," in *International Conference on Ubiquitous Computing*, Springer, pp. 109–126 (available at http://link.springer.com/chapter/10.1007/978-3-540-74853-3_7).

Brustein, J. 2012. "Start-Ups Aim to Help Users Put a Price on Their Personal Data," *NYTimes.com*, New York, NY, USA, p. B3.

Bundesamt für Sicherheit in der Informationstechnik. 2016. "BSI - Akkreditierte De-Mail Diensteanbieter," *Akkreditierte De-Mail Dienstanbieter* (available at https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/Akkreditierte_DMDA/Akkreditierte_DMDA_node.html; retrieved November 7, 2016).

Camenisch, J., Fischer-Hübner, S., and Rannenberg, K. (Eds.). 2011. *Privacy and Identity Management for Life*, Berlin, Heidelberg: Springer (available at http://link.springer.com/10.1007/978-3-642-20317-6).

Capra, R., Vardell, E., and Brennan, K. 2014. "File synchronization and sharing: User practices and challenges," *Proceedings of the American Society for Information Science and Technology* (51:1), pp. 1–10 (doi: 10.1002/meet.2014.14505101059).

Carroll, E., Romano, J., and Gallaga, O. L. 2010. *Your Digital Afterlife: When Facebook, Flickr and Twitter Are Your Estate, What's Your Legacy?*, Berkeley, CA : London: New Riders Publ.

Case, D. 2007. *Looking for information: a survey of research on information seeking, needs, and behavior.* (2 ed.), Amsterdam: Elsevier.

Castelnovo, W. 2016. "Citizens as sensors/information providers in the co-production of smart city services," in *Re-shaping Organizations through Digital and Social Innovation. Proceedings of the 12th Annual Conference of ITAIS*R. Agrifoglio, L. Caporarello, M. Magni, and S. Za (eds.), LUISS University Press, pp. 52–62 (available at https://www.researchgate.net/profile/Walter_Castelnovo/publication/305768274_Citizens_as_sensorsinformation_providers_in_the_co-production_of_smart_city_services/links/57a049ab08aece1c7215ad08.pdf).

Cavoukian, A. 2009. *Privacy by Design... take the Challenge*, Ontario, Canada: Information and Privacy Commissioner of Ontario Canada (available at http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf).

Cecez-Kecmanovic, D., Galliers, R. D., Henfridsson, O., Newell, S., and Vidgen, R. 2014. "The sociomateriality of information systems: current status, future directions," *MIS Quarterly* (38:3), pp. 809–830.

Chin, W. W., Johnson, N., and Schwarz, A. 2008. "A Fast Form Approach to Measuring Technology Acceptance and Other Constructs," *MIS Quarterly* (32:4), pp. 687–703.

Ciampa, M., Revels, M., and Enamait, J. 2011. "Online Versus Local Password Management Applications: An Analysis of User Training and Reactions," *Journal of Applied Security Research* (6:4), pp. 449–466 (doi: 10.1080/19361610.2011.604070).

Cole, C., and Leide, J. 2006. "A Cognitive Framework for Human Information Behavior: The Place of Metaphor in Human Information Organizing Behavior," in *New Directions in Human Information Behavior.* Information Science and Knowledge Management, A. Spink and C. Cole (eds.) (Vol. 8), Springer Netherlands, pp. 171–202 (available at http://www.springerlink.com/content/n7u8527161k52685/abstract/).

CS Transform. 2010. "Citizen Service Transformation: A manifesto for change in the delivery of public services," (available at http://www.cstransform.com/resources/white_papers/CitizenServiceTransformationV1.pdf).

Cushing, A. L. 2012. "Possessions and self extension in digital environments: implications for maintaining personal information," University of North Carolina at Chapel Hill.

Daft, R. L., and Lengel, R. H. 1986. "Organizational Information Requirements, Media Richness and Structural Design," *Management Science* (32:5), pp. 554–571 (doi: 10.1287/mnsc.32.5.554).

Davenport, T. H., and Prusak, L. 1997. *Information Ecology: Mastering the Information and Knowledge Environment* (1st ed.), Oxford University Press.

Dearman, D., and Pierce, J. S. 2008. "It's on my other computer!: computing with multiple devices," in *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, New York, NY, USA: ACM, pp. 767–776 (doi: 10.1145/1357054.1357177).

Deng, T., and Feng, L. 2011. "A survey on information re-finding techniques," *International Journal of Web Information Systems* (7:4), pp. 313–332 (doi: 10.1108/17440081111187538).

Dhillon, G. S., Weerakkody, V., and Dwivedi, Y. K. 2008. "Realising transformational stage e-government: a UK local authority perspective,"

Electronic Government, an International Journal (5:2), pp. 162–180 (doi: 10.1504/EG.2008.016645).

Diefenbach, S., and Hassenzahl, M. 2011. "The dilemma of the hedonic – Appreciated, but hard to justify," *Interacting with Computers* (23:5), pp. 461–472 (doi: 10.1016/j.intcom.2011.07.002).

Duennebeil, S., Sunyaev, A., Leimeister, J. M., and Krcmar, H. 2010. "Strategies for development and adoption of EHR in German ambulatory care," in *Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2010 4th International Conference.*, Presented at the Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2010 4th International Conference. March, pp. 1–8 (doi: 10.4108/ICST.PERVASIVEHEALTH2010.8887).

Ebbers, W. E., Pieterson, W. J., and Noordman, H. N. 2008. "Electronic government: Rethinking channel management strategies," *Government Information Quarterly* (25:2), pp. 181–201 (doi: 10.1016/j.giq.2006.11.003).

e-Boks. 2011. "E-Boks Årsrapport 2010," (available at http://ekstranet.e-boks.dk/files/e-boks_aarsrapport_2010.pdf).

e-Boks. 2016a. "Profile, mission and values," (available at http://www.e-boks.com/corporate/en/about-e-boks/profile-mission-and-values/; retrieved November 18, 2016).

e-Boks. 2016b. "Background," *15 years of success and expansion* (available at https://www.e-boks.com/corporate/en/about-e-boks/background/; retrieved November 7, 2016).

Egelman, S., Brush, A. J., and Inkpen, K. M. 2008. "Family accounts: a new paradigm for user accounts within the home environment," in *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, ACM, pp. 669–678 (available at http://dx.doi.org/10.1145/1460563.1460666).

Elsweiler, D., Baillie, M., and Ruthven, I. 2011. "What makes re-finding information difficult? a study of email re-finding," *Advances in Information Retrieval*, pp. 568–579.

Ericsson. 2012. "Consumer Privacy in an Online World. An Ericsson Consumer Insight Summary Report", Ericsson Consumer Insight,

Stockholm: Ericsson (available at http://www.ericsson.com/res/docs/2012/ericsson_privacy_report_updated_20120203.pdf).

European Commission. 2010. "Towards interoperability for European public services. COM(2010) 744 final.," (available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0744:FIN:EN:PDF).

European Commission. 2012. "eSafe Building Block - Frequently Asked Questions," (available at https://joinup.ec.europa.eu/site/spocs/eSafe/faq.html#general-01; retrieved December 19, 2016).

European Commission. 2014. *Delivering on the European advantage? - "How European governments can and should benefit from innovative public services," eGovernment benchmark: final insight report.*, Luxembourg: Publications Office (available at http://bookshop.europa.eu/uri?target=EUB:NOTICE:KK0114449:EN:HTML).

European Commission. 2016a. "ISA² - Interoperability solutions for public administrations, businesses and citizens," *ISA² - European Commission*, Text, (available at https://ec.europa.eu/isa2/home_en; retrieved December 21, 2016).

European Commission. 2016b. "Defining a common approach to electronic document and file exchange," *ISA² - European Commission*, Text, November 22 (available at https://ec.europa.eu/isa2/actions/defining-common-approach-electronic-document-and-file-exchange_en; retrieved December 21, 2016).

European Commission. 2016c. "Detailed analysis of e-Safe and e-Document solutions in Member States and EU initiatives," unpublished yet, draft obtained through personal communication with Dr. Suzanne Wigard, Program Manager, European Commission, Informatics Directorate-General (DIGIT), Interoperability Solutions for European Public Administrations (ISA) No. SC232DI07171, D03.01, European Commission.

Farnham, S. D., and Churchill, E. F. 2011. "Faceted identity, faceted lives: social and technical issues with being yourself online," in *Proceedings of the ACM 2011 conference on Computer supported cooperative work*.

CSCW '11, New York, NY, USA: ACM, pp. 359–368 (doi: 10.1145/1958824.1958880).

Fidel, R. 2012. *Human Information Interaction: An Ecological Approach to Information Behavior*, MIT Press.

Finger, M., Bukovc, B., and Burhan, M. (Eds.). 2014. *Postal Services in the Digital Age*. Global E-Governance Series (Vol. 6), Amsterdam: IOS Press.

Fischer-Hübner, S., Hoofnagle, C., Krontiris, I., Rannenberg, K., and Waidner, M. 2011. "Online Privacy: Towards Information Self-Determination on the Internet," Dagstuhl Manifesto, Dagstuhl: Dagstuhl Workshop (available at http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf).

Fitzgerald, C. A., Flood, P. C., O'Regan, P., and Ramamoorthy, N. 2008. "Governance structures and innovation in the Irish Software Industry," *The Journal of High Technology Management Research* (19:1), pp. 36–44.

Fredette, S. L. 1995. "Breast cancer survivors: concerns and coping," *Cancer Nursing* (18:1), pp. 35–46.

Giaccardi, E. 2011. "Things We Value," *interactions* (18:1), pp. 17–21 (doi: 10.1145/1897239.1897245).

Girard, T., Korgaonkar, P., and Silverblatt, R. 2003. "Relationship of type of product, shopping orientations, and demographics with preference for shopping on the Internet," *Journal of Business and Psychology* (18:1), pp. 101–120.

Glaser, B. G., and Strauss, A. L. 2009. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Transaction Publishers.

Goffman, E. 1959. *The presentation of self in everyday life*. A Doubleday Anchor book, Garden City, N.Y: Doubleday.

Görg, S., and Bergmann, R. 2015. "Social workflows—Vision and potential study," *Information Systems* (50), pp. 1–19 (doi: 10.1016/j.is.2014.12.007).

Grimm, C., and Chiasson, S. 2014. "Survey on the fate of digital footprints after death," Carleton University, Technical Report TR-14-01, Jan. 2014. (available at https://cs.carleton.ca/sites/default/files/tr/TR-14-01.pdf).

Grönroos, C. 2008. "Service logic revisited: who creates value? And who co-creates?," *European Business Review* (20:4), pp. 298–314 (doi: 10.1108/09555340810886585).

Grönroos, C. 2011. "Value co-creation in service logic: A critical analysis," *Marketing Theory* (11:3), pp. 279–301.

Groza, T., Handschuh, S., and Moeller, K. 2007. "The nepomuk project-on the way to the social semantic desktop," (available at http://ir.library.nuigalway.ie/xmlui/handle/10379/437).

Gruning, J., and Lindley, S. 2016. "Things We Own Together: Sharing Possessions at Home," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI '16, New York, NY, USA: ACM, pp. 1176–1186 (doi: 10.1145/2858036.2858154).

Gulotta, R., Gerritsen, D. B., Kelliher, A., and Forlizzi, J. 2016. "Engaging with Death Online: An Analysis of Systems That Support Legacy-Making, Bereavement, and Remembrance," in *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. DIS '16, New York, NY, USA: ACM, pp. 736–748 (doi: 10.1145/2901790.2901802).

Gulotta, R., Odom, W., Forlizzi, J., and Faste, H. 2013. "Digital Artifacts As Legacy: Exploring the Lifespan and Value of Digital Data," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 1813–1822 (doi: 10.1145/2470654.2466240).

Gwizdka, J. 2004. "Email task management styles: the cleaners and the keepers," in *CHI '04 extended abstracts on Human factors in computing systems*. CHI EA '04, New York, NY, USA: ACM, pp. 1235–1238 (doi: 10.1145/985921.986032).

Ha, A. 2014. "Manilla, The Hearst-Backed Service For Managing Bills, Is Shutting Down On July 1," *TechCrunch*, May 9 (available at http://social.techcrunch.com/2014/05/09/manilla-shuts-down/; retrieved November 7, 2016).

Hagel III, J., and Rayport, J. F. 1997. "The Coming Battle for Customer Information," *Harvard Business Review* (January-February Reprint Number), pp. 5–11.

Hagel, J., and Singer, M. 1999. *Net worth: shaping markets when customers make the rules*, Boston: Harvard Business School Press.

Hanekop, H. 2008. "Die Herausbildung neuer Nutzungsformen von IuK-Technologien: ein empirisches Forschungsdesign basierend auf Nutzungsexperimenten,"K.-S. Rehberg (ed.), Frankfurt am Main: Campus Verl., pp. 1980–1989 (available at http://nbn-resolving.de/urn:nbn:de:0168-ssoar-152252).

Hardjono, T., and Seberry, J. 1996. "Design and security issues in strongbox systems for the internet," *Faculty of Informatics - Papers* (available at http://ro.uow.edu.au/infopapers/1134).

Hassenzahl, M. 2010. "Experience Design: Technology for All the Right Reasons," *Synthesis Lectures on Human-Centered Informatics* (3:1), pp. 1–95 (doi: 10.2200/S00261ED1V01Y201003HCI008).

Hawkins, D. T., and Kahle, B. 2013. *Personal Archiving: Preserving Our Digital Heritage*, Medford, New Jersey: Information Today Inc.

Hayashi, E., and Hong, J. 2013. "'It's Hidden in My Computer': Exploring Account Management Tools and Behaviors (CMU-CyLab-13-007)," Carnegie Mellon University (available at http://repository.cmu.edu/cylab/118).

Heath, W., Alexander, D., and Booth, P. 2013. "Digital Enlightenment, Mydex, and Restoring Control over Personal Data to the Individual," in *Digital enlightenment yearbook 2013: the value of personal data*. M. Hildebrandt, K. O'Hara, and M. Waidner (eds.), Amsterdam: IOS Press, pp. 253–269 (available at http://ebooks.iospress.nl/isbn/978-1-61499-295-0).

Henderson, S. 2009. "How do people manage their documents?: an empirical investigation into personal document management practices among knowledge workers," Thesis PhD--University of Auckland2009.

Hess, P. D. T., Legner, P. D. C., Esswein, P. D. W., Maaß, P. D. W., Matt, D. C., Österle, P. D. H., Schlieter, D. H., Richter, P., and Zarnekow, P. D. R. 2014. "Digital Life as a Topic of Business and Information Systems Engineering?," *Business & Information Systems Engineering*, pp. 1–7 (doi: 10.1007/s12599-014-0332-6).

Hevner, A. R. 2007. "A three cycle view of design science research," *Scandinavian Journal of Information Systems* (19:2), p. 4.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design science in information systems research," *MIS Quarterly*, pp. 75–105.

Hicks, B. J., Dong, A., Palmer, R., and Mcalpine, H. C. 2008. "Organizing and managing personal electronic files: A mechanical engineer's perspective," *ACM Trans. Inf. Syst.* (26:4), p. 23:1–23:40 (doi: 10.1145/1402256.1402262).

Hildebrand, D. 2015. "E-invoicing as the Principal Driver of Change in B2X Letter Market Definitions," in *Postal and Delivery Innovation in the Digital Economy*. M. A. Crew and T. J. Brennan (eds.), Cham: Springer International Publishing, pp. 277–289 (available at http://link.springer.com/10.1007/978-3-319-12874-0_21).

Hopkins, J. P. 2013. "Afterlife in the Cloud: Managing a Digital Estate," *Hastings and Science Technology Law Journal* (210:5), pp. 209–244.

International Post Corporation. 2015. "Global Postal Industry Report 2015 - Key Findings," International Post Corporation (available at https://www.ipc.be/~/media/documents/public/markets/mi%20products/ipc_gpir2015_key_findings.pdf).

Jacobs, E. (n.d.). "Dealing with the digital afterlife - FT.com," (available at http://www.ft.com/cms/s/0/6d532245c-3653-11e3-8ae3-00144feab7de.html#axzz2pdfzpdj9; retrieved January 6, 2014).

Janssen, M., and Estevez, E. 2013. "Lean government and platform-based governance - Doing more with less," *Government Information Quarterly*. ICEGOV 2011 Supplement (30, Supplement 1), pp. S1–S8 (doi: 10.1016/j.giq.2012.11.003).

Jones, W. 2012. *The Future of Personal Information Management, Part 1: Our Information, Always and Forever*, Morgan & Claypool (available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6813158).

Jones, W. 2013. *Transforming Technologies to Manage Our Information: The Future of Personal Information Management, Part 2*Synthesis Lectures on Information Concepts, Retrieval, and Services, Morgan & Claypool (available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6812958).

Jones, W. 2015. *Building a Better World with Our Information: The Future of Personal Information Management, Part 3*, Morgan & Claypool (available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7240060).

Jones, W., and Anderson, K. M. 2011. "Many views, many modes, many tools ... one structure: Towards a Non-disruptive Integration of Personal Information," in *Proceedings of the 22nd ACM conference on Hypertext and hypermedia*. HT '11, New York, NY, USA: ACM, pp. 113–122 (doi: 10.1145/1995966.1995984).

Jones, W., and Bruce, H. 2005. "A Report on the NSF-Sponsored Workshop on Personal Information Management, Seattle, WA, 2005," (available at http://pim.ischool.washington.edu/final%20PIM%20report.pdf).

Jones, W. P. 2008. *Keeping found things found: the study and practice of personal information management*, Morgan Kaufmann.

Jones, W., and Teevan, J. (Eds.). 2007a. *Personal Information Management*, Univ. of Washington Pr.

Jones, W., and Teevan, J. 2007b. *Personal Information Management*, University of Washington Press.

Jung, H., Stolterman, E., Ryan, W., Thompson, T., and Siegel, M. 2008. "Toward a Framework for Ecologies of Artifacts: How Are Digital Artifacts Interconnected Within a Personal Life?," in *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges*. NordiCHI '08, New York, NY, USA: ACM, pp. 201–210 (doi: 10.1145/1463160.1463182).

Kairam, S., Brzozowski, M., Huffaker, D., and Chi, E. 2012. "Talking in Circles: Selective Sharing in Google+," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '12, New York, NY, USA: ACM, pp. 1065–1074 (doi: 10.1145/2207676.2208552).

Kaplan, B., and Maxwell, J. 2005. "Qualitative research methods for evaluating computer information systems," *Evaluating the Organizational Impact of Healthcare Information Systems*, pp. 30–55.

Kaptelinin, V. 2016. "Making the Case for an Existential Perspective in HCI Research on Mortality and Death," in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA '16, New York, NY, USA: ACM, pp. 352–364 (doi: 10.1145/2851581.2892585).

Karger, D. R. 2007. "Unify Everything: It's all the Same to Me," in *Personal Information Management*. W. P. Jones and J. Teevan (eds.), University of Washington Press, pp. 127–152.

Karger, D. R., Bakshi, K., Huynh, D., Quan, D., and Sinha, V. 2005. "Haystack: A Customizable General-Purpose Information Management Tool for End Users of Semistructured Data," in *In CIDR*.

Kaye, J. J., McCuistion, M., Gulotta, R., and Shamma, D. A. 2014. "Money talks: tracking personal finances," ACM Press, pp. 521–530 (doi: 10.1145/2556288.2556975).

Kaye, J. "Jofish." 2011. "Self-reported Password Sharing Strategies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 2619–2622 (doi: 10.1145/1978942.1979324).

Kaye, J. "Jofish," Vertesi, J., Avery, S., Dafoe, A., David, S., Onaga, L., Rosero, I., and Pinch, T. 2006. "To have and to hold: exploring the personal archive," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, New York, NY, USA: ACM, pp. 275–284 (doi: 10.1145/1124772.1124814).

Kemppainen, L. 2016. "Business models for platform operators in MyData based ecosystem–context preventive healthcare," Master's Thesis, University of Oulu (available at https://www.researchgate.net/profile/Laura_Kemppainen/publication/302970557_Business_models_for_platform_operators_in_MyData_based_ecosystem_-_context_preventive_healthcare/links/5734840c08ae298602debc00.pdf).

Khatibloo, F. 2011. "Personal identity management," Forrester Research.

Kim, S. 2013. "Personal digital archives: preservation of documents, preservation of self," Doctoral thesis, University of Texas (available at http://repositories.lib.utexas.edu/handle/2152/21134).

King, R. C., Sen, R., D'Aubeterre, F., and Sethi, V. 2010. "A Trade Value Perspective on Ecommerce Research: An Integration of Transaction Value and Transaction Cost Theories," *Int. J. E-Bus. Res.* (6:2), pp. 59–77 (doi: 10.4018/jebr.2010040104).

King, S., and Cotterill, S. 2007. "Transformational Government? The role of information technology in delivering citizen-centric local public services," *Local Government Studies* (33:3), pp. 333–354 (doi: 10.1080/03003930701289430).

Kirk, D. S., and Sellen, A. 2010. "On human remains," *ACM Transactions on Computer-Human Interaction* (17:3), pp. 1–43 (doi: 10.1145/1806923.1806924).

Klein, H. K., and Myers, M. D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1), p. 67 (doi: 10.2307/249410).

Koehne, B., Shih, P. C., and Olson, J. S. 2012. "Remote and Alone: Coping with Being the Remote Member on the Team," in *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*. CSCW '12, New York, NY, USA: ACM, pp. 1257–1266 (doi: 10.1145/2145204.2145393).

Kohlborn, T., Korthaus, A., Peters, C., and Fielt, E. 2013. "A Comparative Study of Governmental One-Stop Portals for Public Service Delivery:," *International Journal of Intelligent Information Technologies* (9:3), pp. 1–19 (doi: 10.4018/jiit.2013070101).

Kubicek, H., and Noack, T. 2010. *Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis? Der neue Personalausweis im europäischen Vergleich*, Münster: LIT.

Kuneva, M. 2009. "EUROPA - Press Releases - Meglena Kuneva, European Consumer Commissioner, Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling , Brussels, 31 March 2009," (available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/156; retrieved June 10, 2012).

Kuppinger, M. 2012a. "Advisory Note: Life Management Platforms: Control and Privacy for Personal Data," No. 70608, (available at http://www.kuppingercole.com/report/advisorylifemanagementplatforms70608l3412).

Kuppinger, M. 2012b. "Intention and Attention – how Life Management Platforms can improve Marketing | Martin Kuppinger," May 15 (available at http://blogs.kuppingercole.com/kuppinger/2012/05/15/intention-and-attention-how-life-management-platforms-can-improve-marketing/; retrieved June 8, 2012).

Kuppinger, M., and Kearns, D. 2013. "Life Management Platforms: Control and Privacy for Personal Data," in *Digital enlightenment yearbook 2013: the value of personal data* M. Hildebrandt, K. O'Hara, and M.

Waidner (eds.), Amsterdam: IOS Press, pp. 243–252 (available at http://ebooks.iospress.nl/isbn/978-1-61499-295-0).
Küstenmacher, W. T. 2004. *How to Simplify Your Life: Seven Practical Steps to Letting Go of Your Burdens and Living a Happier Life* (1st ed.), McGraw-Hill.
Kuutti, K. 2013. "'Practice turn' and CSCW identity," *ECSCW 2013 Adjunct Proceedings* (available at http://ojs.statsbiblioteket.dk/index.php/daimipb/article/download/13587/11586#page=47).
Kvavilashvili, L., and Ellis, J. 2004. "Ecological validity and the real-life/laboratory controversy in memory research: A critical (and historical) review," *History and Philosophy of Psychology* (6), pp. 59–80.
Lazarus, R. S., and Folkman, S. 1984. *Stress, appraisal, and coping*, New York: Springer Publ. Comp.
Lazarus, R. S., and Folkman, S. 1987. "Transactional theory and research on emotions and coping," *European Journal of Personality* (1:3), pp. 141–169 (doi: 10.1002/per.2410010304).
Lee, C. A. 2011. *I, Digital: Personal Collections in the Digital Era*, Amer Library Assn.
Leickly, B. L. 2004. "Intermediaries in Information Economies," Master's Thesis, , Georgetown: Georgetown University (available at http://www8.georgetown.edu/cct/thesis/Bethany_Leickly.pdf).
Lenz, T. 2001. *E-Government und E-Nonprofit. Management von Internetprojekten in Verwaltung und Nonprofit-Organisationen. Netzwert-Edition.*, Schäffer-Poeschel.
Levy, Y., and Ellis, T. J. 2006. "A systems approach to conduct an effective literature review in support of information systems research," *Informing Science: International Journal of an Emerging Transdiscipline* (9), pp. 181–212.
Liang, T.-P., and Huang, J.-S. 1998. "An empirical study on consumer acceptance of products in electronic markets: a transaction cost model," *Decision Support Systems* (24:1), pp. 29–43 (doi: 10.1016/S0167-9236(98)00061-X).
Liu, C., and Arnett, K. P. 2000. "Exploring the factors associated with Web site success in the context of electronic commerce," *Information & Management* (38:1), pp. 23–33 (doi: 10.1016/S0378-7206(00)00049-5).

von Lucke, J. 2005. "Vision eines elektronischen Dokumentensafes," in: S. Klewitz-Hommelsen and Hinrich Bonin (eds.), *Die Zeit nach E-Government, Buchreihe E-Government und die Erneuerung des öffentlichen Sektors*, Band 2, Münster: LIT Verlag, pp. 109–129.

von Lucke, J. 2007. "Portals for the public sector," in *Encyclopedia of Digital Government* A.-V. Anttiroiko and M. Malkia (eds.), IGI Global, pp. 1328–1333 (available at http://www.igi-global.com/chapter/portals-public-sector/11677).

von Lucke, J. 2008. „Hochleistungsportale für die öffentliche Verwaltung," *Schriftenreihe Wirtschaftsinformatik, Band 55, Forschungs-bericht, zugleich Habilitationsschrift an der DHV Speyer*, Lohmar and Cologne: Josef Eul Verlag.

von Lucke, J. 2015. "Smart Government - Wie uns die intelligente Vernetzung zum Leitbild „Verwaltung 4.0" und einem smarten Regierungs- und Verwaltungshandeln führt," Whitepaper, The Open Government Institute, Zeppelin Universität Friedrichshafen (available at https://www.zu.de/institute/togi/assets/pdf/ZU-150914-Smart-Government-V1.pdf).

von Lucke, J. 2016a. "Smart Government - The Potential of Intelligent Networking in Government and Public Administration," in *2016 Conference for E-Democracy and Open Government (CeDEM)*, Presented at the 2016 Conference for E-Democracy and Open Government (CeDEM), May, pp. 137–144 (doi: 10.1109/CeDEM.2016.22).

von Lucke, J. 2016b. "Deutschland auf dem Weg zum Smart Government," *Verwaltung & Management* (22:4), pp. 171–186 (doi: 10.5771/0947-9856-2016-4-171).

Lutters, W. G., Ackerman, M. S., and Zhou, X. 2007. "Group Information Management," in *Personal Information Management*. W. Jones and J. Teevan (eds.), Seattle and London: University of Seattle Press, pp. 236–248 (available at https://www.researchgate.net/profile/Wayne_Lutters/publication/228748005_14_Group_Information_Management/links/ofcfd50d1cf6c01c41000000.pdf).

Maciel, C., and Pereira, V. C. 2015. "Post-mortem Digital Legacy: Possibilities in HCI," in *Human-Computer Interaction: Users and Contexts*. Lecture Notes in Computer Science, M. Kurosu (ed.), Springer International Publishing, pp. 339–349 (doi: 10.1007/978-3-319-21006-3_33).

Maier, C. 2014. "Technostress: Theoretical foundation and empirical evidence," Otto-Friedrich-Universität Bamberg, Diss., 2014: Universität Bamberg (available at http://nbn-resolving.de/urn:nbn:de:bvb:473-opus4-256587).

Maier, C., Laumer, S., Eckhardt, A., and Weitzel, T. 2012. "Online Social Networks as a Source and Symbol of Stress: An Empirical Analysis," *ICIS 2012 Proceedings* (available at http://aisel.aisnet.org/icis2012/proceedings/DigitalNetworks/10).

Maier, C., Laumer, S., Eckhardt, A., and Weitzel, T. 2014. "Giving too much social support: social overload on social networking sites," *European Journal of Information Systems* (24:5), pp. 447–464 (doi: 10.1057/ejis.2014.3).

Malone, T. W. 1983. "How do people organize their desks?: Implications for the design of office information systems," *ACM Trans. Inf. Syst.* (1:1), pp. 99–112 (doi: 10.1145/357423.357430).

Marshall, C. 2007. "How people manage personal information over a lifetime," in *Personal Information Management*. W. Jones and J. Teevan (eds.), Univ of Washington Press, pp. 153–166.

Marshall, C. 2008a. "Rethinking Personal Digital Archiving, Part 1," *D-Lib Magazine* (14:3/4) (doi: 10.1045/march2008-marshall-pt1).

Marshall, C. 2008b. "Rethinking Personal Digital Archiving, Part 2," *D-Lib Magazine* (14:3/4) (doi: 10.1045/march2008-marshall-pt2).

Marshall, C. 2011. "Challenges and Opportunities for Personal Digital Archiving," in *Personal Collections in the Digital Era*, Chicago, IL: Society of American Archivists, pp. 90–114 (available at http://www.csdl.tamu.edu/~marshall/I-Digital-Marshall.pdf).

Marshall, C., Bly, S., and Brun-Cottan, F. 2007. "The long term fate of our digital belongings: Toward a service model for personal archives," *arXiv preprint arXiv:0704.3653* (available at http://arxiv.org/abs/0704.3653).

Marshall, C., and Tang, J. C. 2012. "That syncing feeling: early user experiences with the cloud," in *Proceedings of the Designing Interactive Systems Conference*, New York, NY, USA: ACM, pp. 544–553 (doi: 10.1145/2317956.2318038).

Massimi, M., and Charise, A. 2009. "Dying, death, and mortality: towards thanatosensitivity in HCI," in *CHI'09 Extended Abstracts on Human*

Factors in Computing Systems, pp. 2459–2468 (available at http://dl.acm.org/citation.cfm?id=1520349).

Massimi, M., Dimond, J. P., and Le Dantec, C. A. 2012. "Finding a new normal: the role of technology in life disruptions," in *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*. CSCW '12, New York, NY, USA: ACM, pp. 719–728 (doi: 10.1145/2145204.2145314).

Massimi, M., Odom, W., Banks, R., and Kirk, D. 2011. "Matters of life and death: locating the end of life in lifespan-oriented hci research," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '11, New York, NY, USA: ACM, pp. 987–996 (doi: 10.1145/1978942.1979090).

Matthews, T., Liao, K., Turner, A., Berkovich, M., Reeder, R., and Consolvo, S. 2016. "'She'll Just Grab Any Device That's Closer': A Study of Everyday Device & Account Sharing in Households," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI '16, New York, NY, USA: ACM, pp. 5921–5932 (doi: 10.1145/2858036.2858051).

Mayer-Schönberger, V. 2007. "Useful void: The art of forgetting in the age of ubiquitous computing," *KSG Working Paper No. RWP07-022*.

McDermott, A. 2016. "Don't Let It Happen to You: Avoid These Business Killers With a Prepared Marketing Plan," *Business.com*, February 11 (available at http://www.business.com/marketing/avoid-these-business-killers-with-a-prepared-marketing-plan/; retrieved November 7, 2016).

McKemmish, S. 2001. "Placing records continuum theory and practice," *Archival science* (1:4), pp. 333–359.

McKemmish, S., and Piggott, M. 1994. *The records continuum: Ian Maclean and Australian Archives: first fifty years*, Clayton: Ancora Press.

Meyer-Jäkel, D. 2011. *doMap- Kontinuierliche Weiterentwicklung des virtuellen Rathauses Stadt Dortmund*, Presented at the CeBIT, Hannover.

Moncur, W., Gibson, L., and Herron, D. 2016. "The Role of Digital Technologies During Relationship Breakdowns," ACM Press, pp. 370–381 (doi: 10.1145/2818048.2819925).

Moncur, W., and Kirk, D. 2014. "An Emergent Framework for Digital Memorials," in *Proceedings of the 2014 Conference on Designing Interactive Systems*. DIS '14, New York, NY, USA: ACM, pp. 965–974 (doi: 10.1145/2598510.2598516).

Müller, L.-S. 2011. "Lebenslagen zur Strukturierung von Bürgerservices," in *Bürgerservices : Grundlagen, Ausprägungen, Gestaltung, Potenziale*. E-Government und die Erneuerung des öffentlichen Sektors, G. Schwabe (ed.), Berlin: Edition Sigma, pp. 71–96.

Mun, M., Hao, S., Mishra, N., Shilton, K., Burke, J., Estrin, D., Hansen, M., and Govindan, R. 2010. "Personal data vaults: a locus of control for personal data streams," in *Proceedings of the 6th International Conference*. Co-NEXT '10, New York, NY, USA: ACM, p. 17:1–17:12 (doi: 10.1145/1921168.1921191).

Mydex. 2009. "The Case for Personal Information Empowerment - The rise of the personal data store.," Mydex (available at http://mydex.org/wp-content/uploads/2010/09/The-Case-for-Personal-Information-Empowerment-The-rise-of-the-personal-data-store-A-Mydex-White-paper-September-2010-Final-web.pdf).

Myers, M. D. 1997. "Qualitative Research in Information Systems," *MIS Quarterly* (21:2), p. 241 (doi: 10.2307/249422).

Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., and Boneh, D. 2012. "A Critical Look at Decentralized Personal Data Architectures," *arXiv:1202.4503* (available at http://arxiv.org/abs/1202.4503).

Nardi, B. A., and O'Day, V. L. 2000. *Information ecologies: using technology with heart* (1. MIT Press paperback ed.), Cambridge, Mass.: MIT Press.

@niral89, @mmazco, and milc.co. 2016. "Autopsy - Lessons from Failed Startups," *Autopsy*, November 7 (available at http://autopsy.io/; retrieved November 7, 2016).

Nissenbaum, H. F. 2010. *Privacy in context: technology, policy, and the integrity of social life*, Stanford, Calif.: Stanford Law Books.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126 (doi: 10.1111/j.1745-6606.2006.00070.x).

North, K. 2016. *Wissensorientierte Unternehmensführung: Wissensmanagement gestalten* (6., und erw. Aufl. 2016.), Wiesbaden: Springer Fachmedien Wiesbaden.

Nussbaumer, P., and Matter, I. 2011. "What You See Is What You (Can) Get? Designing for Process Transparency in Financial Advisory Encounters," in *Human-Computer Interaction – INTERACT 2011*P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque, and M. Winckler (eds.) (Vol. 6946), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 277–294 (available at http://www.springerlink.com/index/10.1007/978-3-642-23774-4_24).

OASIS. 2014. "Transformational Government Framework Version 2.0," (available at http://docs.oasis-open.org/tgf/TGF/v2.0/TGF-v2.0.html; retrieved December 22, 2016).

Odom, W., Banks, R., Kirk, D., Harper, R., Lindley, S., and Sellen, A. 2012. "Technology heirlooms?: considerations for passing down and inheriting digital materials," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '12, New York, NY, USA: ACM, pp. 337–346 (doi: 10.1145/2207676.2207723).

Odom, W., Sellen, A., Harper, R., and Thereska, E. 2012. "Lost in translation: understanding the possession of digital things in the cloud," in *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, pp. 781–790 (doi: 10.1145/2207676.2207789).

Orlikowski, W. J., and Baroudi, J. J. 1991. "Studying information technology in organizations: Research approaches and assumptions," *Information systems research* (2:1), pp. 1–28.

Osterwalder, A. 2004. "The business model ontology: A proposition in a design science approach," Université de Lausanne.

Osterwalder, A., and Pigneur, Y. 2010. *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers* (1. Auflage.), John Wiley & Sons.

Papadomichelaki, X., Magoutas, B., Halaris, C., Apostolou, D., and Mentzas, G. 2006. "A review of quality dimensions in e-government services," in *Proceedings of the 5th international conference on Electronic Government*EGOV'06, Berlin, Heidelberg: Springer-Verlag, pp. 128–138 (doi: 10.1007/11823100_12).

Parisopoulos, K., Tambouris, E., and Tarabanis, K. 2014. "An investigation of national policies on transformational government (t-Gov) in Europe," *International Journal of Information Technology and Management* (13:4), pp. 305–323 (doi: 10.1504/IJITM.2014.065628).

Parker, G., Van Alstyne, M., and Choudary, S. P. 2016. *Platform revolution: how networked markets are transforming the economy and how to make them work for you* (First Edition.), New York: W. W. NORTON & COMPANY.

Pavlou, P. A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly* (35:4), pp. 977–988.

Peduzzi, A. R. 2013. "Design und Evaluation einer Applikation zur Unterstützung der mobilen Erfassung persönlicher Informationen," Master's Thesis, Zürich: University of Zurich (available at http://www.merlin.uzh.ch/publication/show/8792).

Pentland, A. 2009. "Reality mining of mobile communications: Toward a new deal on data," *The Global Information Technology Report 2008–2009*, p. 1981.

Peoples, C., and Hetherington, M. 2015. "The cloud afterlife: Managing your digital legacy," in *2015 IEEE International Symposium on Technology and Society (ISTAS)*, Presented at the 2015 IEEE International Symposium on Technology and Society (ISTAS), November, pp. 1–7 (doi: 10.1109/ISTAS.2015.7439412).

Pfister, J. 2017. "'This will cause a lot of work.' – Coping with Transferring Files and Passwords as Part of a Personal Digital Legacy," in *Proceedings of 20th ACM Conference on Computer-Supported Cooperative Work and Social Computing*, Presented at the 20th ACM Conference on Computer-Supported Cooperative Work and Social Computing, Portland, Oregon, United States.

Pfister, J., and Schwabe, G. 2013. "The Landscape of Electronic Data Safes and Their Adoption in E-Government and E-Business," in *2013 46th Hawaii International Conference on System Sciences (HICSS)*, Presented at the 2013 46th Hawaii International Conference on System Sciences (HICSS), pp. 1963–1972 (doi: 10.1109/HICSS.2013.532).

Pfister, J., and Schwabe, G. 2015. "Electronic Data Safes as an Infrastructure for Transformational Government? A Case Study," in *Electronic*

Government, 14th IFIP WG 8.5 International Conference, EGOV 2015, Thessaloniki, Greece, Proceedings. E. Tambouris, M. Janssen, H. J. Scholl, M. A. Wimmer, K. Tarabanis, M. Gascó, B. Klievink, I. Lindgren, and P. Parycek (eds.), Springer International Publishing, pp. 246–257 (doi: 10.1007/978-3-319-22479-4_19).

Pfister, J., and Schwabe, G. 2016. "Going Paperless with Electronic Data Safes: Information Ecology Fit and Challenges," in *Proceedings of the Thirty Seventh International Conference on Information Systems 2016*, Presented at the Thirty Seventh International Conference on Information Systems 2016, Dublin, in press.

Prates, R. O., Rosson, M. B., and Souza, C. S. de. 2015. "Making Decisions About Digital Legacy with Google's Inactive Account Manager," in *Human-Computer Interaction – INTERACT 2015*Lecture Notes in Computer Science, J. Abascal, S. Barbosa, M. Fetter, T. Gross, P. Palanque, and M. Winckler (eds.), Springer International Publishing, pp. 201–209 (doi: 10.1007/978-3-319-22701-6_14).

Project VRM. 2012. "Main Page - Project VRM," (available at http://cyber.law.harvard.edu/projectvrm/Main_Page; retrieved February 6, 2012).

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., and Tu, Q. 2008. "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation," *Information Systems Research* (19:4), pp. 417–433 (doi: 10.1287/isre.1070.0165).

Reber, D. L. 2013. "Design und Evaluation einer webbasierten Personal Life Management Applikation," Master's Thesis, Zürich: University of Zurich (available at http://www.merlin.uzh.ch/publication/show/8792).

Reed, D., Johnston, J., and David, S. 2011. "The Personal Network: A New Trust Model and Business Model for Personal Data," Connect.Me (available at http://openidentityexchange.org/sites/default/files/the-personal-network-whitepaper.pdf).

Rosson, M. B., and Carroll, J. M. 2002. *Usability engineering: scenario-based development of human-computer interaction*. The Morgan Kaufmann series in interactive technologies, San Francisco [etc.]: Morgan Kaufmann.

Rudland, G. 2012. "Safety net," *Exceptional Netherlands* (January-June 2012), pp. 4–9.

Salo, M., Makkonen, M., and Hekkala, R. 2015. "'I just cursed and opened a beer': Explaining Mobile Users' Non-Complaining Behavior Through Coping," in *Proceedings of the Thirty Sixth International Conference on Information Systems - Exploring the Information Frontier*, Presented at the ICIS 2015, Fort Worth, USA (available at http://aisel.aisnet.org/icis2015/proceedings/HumanBehaviorIS/12/).

Sauermann, L. 2009. "The Gnowsis Semantic Desktop approach to Personal Information Management," Universität Kaiserslautern (available at http://www.dfki.uni-kl.de/~sauermann/papers/Sauermann2009phd.pdf).

Schatzki, T. R., Knorr-Cetina, K., and Savigny, E. von. 2001. *The practice turn in contemporary theory*, London; New York: Routledge (available at http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=134021).

Scholl, H. J. (Jochen), and Dwivedi, Y. K. 2014. "Forums for electronic government scholars: Insights from a 2012/2013 study," *Government Information Quarterly* (31:2), pp. 229–242 (doi: 10.1016/j.giq.2013.10.008).

Schulz, S., Hoffmann, C., Klessmann, J., Penski, A., and Warnecke, T. 2010. "Dienste auf Basis elektronischer Safes für Daten und Dokumente," Lorenz-von-Stein-Institut, Fraunhofer FOKUS.

Schwabe, G. 2011. "Online-Bürgerservices," in *Bürgerservices Grundlagen - Ausprägungen - Gestaltung - Potentiale.*G. Schwabe (ed.), Berlin: edition sigma, pp. 97–112.

Sellen, A. J., and Harper, R. H. R. 2002. *The myth of the paperless office*, Cambridge, Mass: MIT Press.

Siegel, D. 2009. *Pull: The Power of the Semantic Web to Transform Your Business* (1st ed.), Portfolio Hardcover.

Siegel, D. 2011. "Personal Data Locker Vision," *Personal Data Locker Vision* (available at https://vimeo.com/14061238; retrieved January 19, 2017).

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., and Furlong, M. 2007. "Password Sharing: Implications for Security Design Based on

Social Practice," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '07, New York, NY, USA: ACM, pp. 895–904 (doi: 10.1145/1240624.1240759).

Slone, D. J. 2000. "Encounters with the OPAC: On-line searching in public libraries," *Journal of the American Society for Information Science* (51:8), pp. 757–773 (doi: 10.1002/(SICI)1097-4571(2000)51:8<757::AID-ASI80>3.0.CO;2-T).

Spurgin, K. M. 2008. "Everyday information organization practices in the pursuit of leisure: The information organization, management, and keeping activities of amateur art photographers," (available at http://infomuse.net/papers/litreview.pdf).

Stadt Dortmund. 2004. "E-Government Dortmund - Projekt Digitale Stadtverwaltung.,"

Star, S. L., and Griesemer, J. R. 1989. "Institutional Ecology, `Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39," *Social Studies of Science* (19:3), pp. 387–420 (doi: 10.1177/030631289019003001).

Stein, M. 2014. "FileThis Paperless Fetching Technology Helps Power New Digital Document Delivery Service Platform, Inlet™," *FileThis Paperless Fetching Technology Helps Power New Digital Document Delivery Service Platform, Inlet™*, June 9 (available at https://filethis.com/filethis-paperless-fetching-technology-helps-power-new-digital-document-delivery-service-platform-inlet/; retrieved November 7, 2016).

Stein, N., Folkman, S., Trabasso, T., and Richards, T. A. 1997. "Appraisal and goal processes as predictors of psychological well-being in bereaved caregivers," *Journal of Personality and Social Psychology* (72:4), pp. 872–884 (doi: 10.1037/0022-3514.72.4.872).

Stobert, E., and Biddle, R. 2014. "The password life cycle: user behaviour in managing passwords," in *Proceedings of Tenth Symposium on Usable Privacy and Security*, Presented at the SOUPS, Menlo Park, Ca, USA, pp. 243–255 (available at https://www.usenix.org/system/files/conference/soups2014/soups14-paper-stobert.pdf).

Stobert, E., and Biddle, R. 2015. "Expert Password Management," in *Technology and Practice of Passwords - 9th International Conference*, Presented at the PASSWORDS, Cambridge, UK, pp. 3–20 (available at

https://passwordscon.org/wp-content/uploads/2015/05/preproceedings.pdf).

Stock, W. G., and Stock, M. 2013. *Handbook of Information Science*, Berlin, Boston: De Gruyter Saur (available at https://www.degruyter.com/viewbooktoc/product/174024).

Strauss, A., and Corbin, J. M. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, SAGE.

Strauss, A. L., and Corbin, J. M. 1998. *Basics of qualitative research: techniques and procedures for developing grounded theory* (2nd ed.), Thousand Oaks: Sage Publications.

Tang, J. C., Brubaker, J. R., and Marshall, C. C. 2013. "What Do You See in the Cloud? Understanding the Cloud-Based User Experience through Practices," in *Human-Computer Interaction – INTERACT 2013*Lecture Notes in Computer Science, P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson, and M. Winckler (eds.), Springer Berlin Heidelberg, pp. 678–695 (doi: 10.1007/978-3-642-40480-1_47).

Tanner, A. 2014. *What Stays in Vegas: The World of Personal Data—Lifeblood of Big Business—and the End of Privacy as We Know It* (First Edition.), New York: PublicAffairs.

Tavakoli, A., and Schlagwein, D. 2016. "A REVIEW OF THE USE OF PRACTICE THEORY IN INFORMATION SYSTEMS RESEARCH," in *Proceedings of the Pacific Asia Conference on Information Systems*. P. Y. K. Chau and C. She-I (eds.), Presented at the PACIS, Chiayi, Taiwan (available at www.pacis2016.org/Abstract/ALL/553.pdf).

Teevan, J., Liebling, D. J., and Lasecki, W. S. 2014. "Selfsourcing personal tasks," Presented at the CHI, Toronto, Ontario, Canada: ACM Press, pp. 2527–2532 (doi: 10.1145/2559206.2581181).

Thomson, L. 2013. "'When I've packed it in and they send me something ...': Information boundaries in professional home offices," *Proceedings of the American Society for Information Science and Technology* (50:1), pp. 1–5 (doi: 10.1002/meet.14505001158).

TNS infratest. 2012. "eGovernment Monitor 2012. Nutzung und Akzeptanz von elektronischen Bürgerdiensten im internationalen Vergleich.," (available at http://www.vitako.de/Positionen/externe/Documents/eGovernmentMONITOR2011-D21.pdf).

Tungare, M. 2009. "Mental Workload at Transitions between Multiple Devices in Personal Information Management," (available at http://pimworkshop.org/2009/papers/tungare-pim2009.pdf).

Van Kleek, M. 2011. "Effort, memory, attention and time: paths to more effective personal information management," Thesis, (available at http://dspace.mit.edu/handle/1721.1/66466; retrieved March 8, 2012).

Van Kleek, M., Smith, D., Shadbolt, N., and others. 2012. "A decentralized architecture for consolidating personal information ecosystems: The WebBox.,"

Vargo, S. L., and Lusch, R. F. 2004. "Evolving to a new dominant logic for marketing," *Journal of marketing*, pp. 1–17.

Vargo, S. L., and Lusch, R. F. 2008. "Why 'service'?," *Journal of the Academy of Marketing Science* (36:1), pp. 25–38 (doi: 10.1007/s11747-007-0068-7).

Vargo, S. L., Maglio, P. P., and Akaka, M. A. 2008. "On value and value co-creation: A service systems and service logic perspective," *European management journal* (26:3), pp. 145–152.

Veenstra, A. F. V., Klievink, B., and Janssen, M. 2011. "Barriers and impediments to transformational government: insights from literature and practice," *Electronic Government, an International Journal* (8:2/3), p. 226 (doi: 10.1504/EG.2011.039838).

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems," *MIS Quarterly* (37:1), pp. 21–54.

Venkatesh, V., Morris, M. G., Gordon B. Davis, and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425–478.

Verble, J. 2014. "The NSA and Edward Snowden: Surveillance in the 21st Century," SIGCAS Comput. Soc., (44:3), pp. 14–20 (doi: 10.1145/2684097.2684101).

Vertesi, J., Kaye, J., Jarosewski, S. N., Khovanskaya, V. D., and Song, J. 2016. "Data Narratives: Uncovering Tensions in Personal Data Management," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, New York, NY, USA: ACM, pp. 478–490 (doi: 10.1145/2818048.2820017).

Vincent, C. J., Li, Y., and Blandford, A. 2014. "Integration of human factors and ergonomics during medical device design and development: It's all about communication," *Applied Ergonomics* (45:3), pp. 413–419 (doi: 10.1016/j.apergo.2013.05.009).

Voida, A., Olson, J. S., and Olson, G. M. 2013. "Turbulence in the Clouds: Challenges of Cloud-based Information Work," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '13, New York, NY, USA: ACM, pp. 2273–2282 (doi: 10.1145/2470654.2481313).

Waagstein, A. 2014. "An exploratory study of digital legacy among death aware people," *Thanatos* (3:1), pp. 46–67.

Watkins, R. D., Sellen, A., and Lindley, S. E. 2015. "Digital Collections and Digital Collecting Practices," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI '15, New York, NY, USA: ACM, pp. 3423–3432 (doi: 10.1145/2702123.2702380).

Weerakkody, V., Dhillon, G., Dwivedi, Y., and Currie, W. 2008. "Realising transformational stage e-government: challenges, issues and complexities," *AMCIS 2008 Proceedings*, p. 181.

Weerakkody, V., Janssen, M., and Dwivedi, Y. K. 2011. "Transformational change and business process reengineering (BPR): Lessons from the British and Dutch public sector," *Government Information Quarterly* (28:3), pp. 320–328 (doi: 10.1016/j.giq.2010.07.010).

Wegner, D. M. 1987. "Transactive Memory: A Contemporary Analysis of the Group Mind," in *Theories of Group Behavior*. B. Mullen and G. R. Goethals (eds.), Springer New York, pp. 185–208 (doi: 10.1007/978-1-4612-4634-3_9).

Weitzman, E. R., Kaci, L., and Mandl, K. D. 2009. "Acceptability of a Personally Controlled Health Record in a Community-Based Setting: Implications for Policy and Design," *Journal of Medical Internet Research* (11:2) (doi: 10.2196/jmir.1187).

Whitley, Edgar A. 2009. "Informational privacy, consent and the 'control' of personal data," *Information Security Technical Report* (14:3), pp. 154–159 (doi: 10.1016/j.istr.2009.10.001).

Whittaker, S. 2011. "Personal information management: From information consumption to curation," *Annual Review of Information Science and Technology* (45:1), pp. 1–62 (doi: 10.1002/aris.2011.1440450108).

Wilson, T. D. 2000. "Human information behavior," *Informing science* (3:2), pp. 49–56.

Wimmer, M. A. 2002. "Integrated service modelling for online one-stop government," *Electronic Markets* (12:3), pp. 149–156.

Winckler, M., Gaits, V., Vo, D.-B., Sergio, F., and Rossi, G. 2011. "An approach and tool support for assisting users to fill-in web forms with personal information," in *Proceedings of the 29th ACM international conference on Design of communication*. SIGDOC '11, New York, NY, USA: ACM, pp. 195–202 (doi: 10.1145/2038476.2038515).

World Economic Forum. 2011. "Personal Data: The Emergence of a New Assest Class," (available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf).

World Economic Forum, W. 2012. "Rethinking Personal Data: Strengthening Trust," World Economic Forum (available at http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf).

World Economic Forum, W. 2014. "Rethinking Personal Data: A New Lens for Strengthening Trust," World Economic Forum (available at http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf).

Xie, X., Sonnenwald, D. H., and Fulton, C. 2015. "The role of memory in document re-finding," *Library Hi Tech* (33:1), pp. 83–102 (doi: 10.1108/LHT-06-2014-0050).

Yildiz, M. 2007. "E-government research: Reviewing the literature, limitations, and ways forward," *Government Information Quarterly* (24:3), pp. 646–665 (doi: 10.1016/j.giq.2007.01.002).

Yvette Blount. 2011. "Employee management and service provision: a conceptual framework," *Information Technology & People* (24:2), pp. 134–157 (doi: 10.1108/09593841111137331).

Zolnowski, A. 2015. "Analysis and Design of Service Business Models," Universität Hamburg (available at http://d-nb.info/1075317479).

Zolnowski, A., and Böhmann, T. 2011. "Business modeling for services: Current state and research perspectives," in *AMCIS 2011 Proceedings - All Submissions.*, Presented at the Seventeenth Americas Conference on Information System, Detroit, MI, USA (available at http://aisel.aisnet.org/amics_2011_submissions/394).

Zolnowski, A., and Böhmann, T. 2014. "Formative Evaluation of Business Model Representations – the Service Business Model Canvas," in *Proceedings of the European Conference on Information Systems (ECIS) 2014*, Presented at the Twenty Second European Conference on Information Systems, Tel Aviv, Israel, June 9 (available at http://aisel.aisnet.org/ecis2014/proceedings/track20/8).

Zolnowski, A., Weiß, C., and Böhmann, T. 2014. "Representing Service Business Models with the Service Business Model Canvas – The Case of a Mobile Payment Service in the Retail Industry," in *2014 47th Hawaii International Conference on System Sciences*, Presented at the 2014 47th Hawaii International Conference on System Sciences, January, pp. 718–727 (doi: 10.1109/HICSS.2014.96).

8 List of Figures

9 List of Tables